The Shield

CyberSecurity Dossier 2020•21

Optimising investments to reduce overall risk

future. perfect. simple.

The Shield

CyberSecurity Dossier 2020•21

Optimising investments to reduce overall risk

Sommario

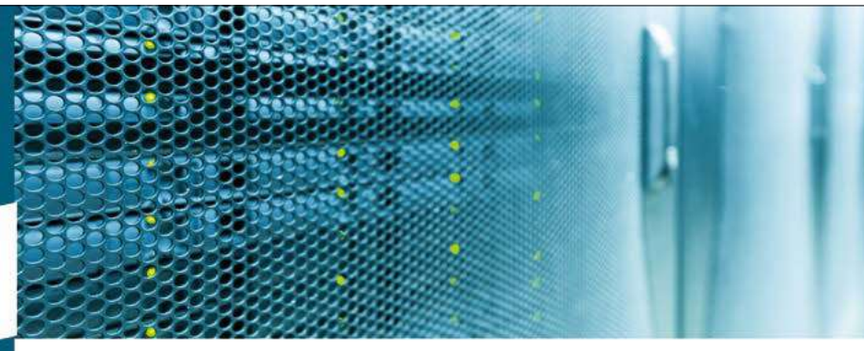
contattaesperto@exprivia.com

www.exprivia.com

Visione e strategia sulla Cybersecurity

exprivia

future. perfect. simple.



CyberSecurity

Ottimizzare gli investimenti per ridurre il rischio complessivo

Ridurre il rischio di un attacco e limitare i danni di un incidente di sicurezza

In un mondo popolato da dispositivi intelligenti interconnessi, dove il dato è il vero carburante su cui si basa l'innovazione e le nuove tecnologie prendono spesso il sopravvento sulla capacità di governarle, la sicurezza e la gestione della privacy diventano un fattore abilitante, aventi **valore intrinseco**.
La sicurezza non è più vincolata solo al servizio a cui è funzionale o all'asset necessario per erogarlo, ma è necessaria a **sostenere l'intero processo di digitalizzazione**. Gli investimenti pertanto non possono essere solo in funzione del ritorno economico, ma vanno fatti con la presa di coscienza che la non-sicurezza del singolo dispositivo intelligente può trasformarsi nella **non-sicurezza dell'intero pianeta digitale**. Strategia questa ben nota agli attaccanti che oggi non sono solo interessati a compromettere un servizio, ma anche a catturare i dispositivi che verranno utilizzati come sorgente per successivi attacchi senza creare alcun danno al legittimo proprietario, spesso inconsapevole.
È necessaria una **modifica culturale** e una presa di coscienza rapida su quelli che sono i rischi di un incidente in ambito sicurezza: **mancanza di cultura e consapevolezza** sono le vulnerabilità più spesso sfruttate dagli attaccanti, prima ancora che vulnerabilità sul software o sull'hardware.
Infine, la **distanza tra risorse di tempo, denaro e professionalità** tra chi è specializzato negli attacchi e chi si difende, rende fondamentale ottimizzare gli investimenti per ridurre i rischi e i danni di un attacco.
La strategia Exprivia in ambito CyberSecurity si è sviluppata con l'obiettivo di **supportare i clienti nel processo di trasformazione digitale** rendendolo il più sicuro possibile e **compatibile con i limiti di spesa** e di **conformità a regolamentazioni**. Essa si basa su condivisione delle informazioni, competenza e consapevolezza, servizi di consulenza, attività di protezione, monitoraggio continuo, capacità di rispondere a un attacco e ripristinare il servizio e conoscenza dell'industria in termini di processi e architetture.

exprivia

future. perfect. simple.

Condivisione delle informazioni - La sicurezza è un processo che richiede un adattamento continuo alle tecniche di attacco utilizzate. Exprivia ha creato un Osservatorio che analizza incidenti, attacchi e violazioni della privacy nel territorio italiano che rendere più efficienti i nostri servizi. Crediamo nel valore della condivisione e condividiamo le informazioni ogni tre mesi.

Consapevolezza - La vulnerabilità più spesso sfruttata dagli attaccanti è il fattore umano, la cui mancanza di consapevolezza è la conseguenza di una veloce accelerazione nel processo di digitalizzazione che non ha dato la possibilità di metabolizzare una cultura della sicurezza. Exprivia mette a disposizione corsi di alfabetizzazione sulla CyberSecurity che sono fruibili on demand tramite la piattaforma Udemy.

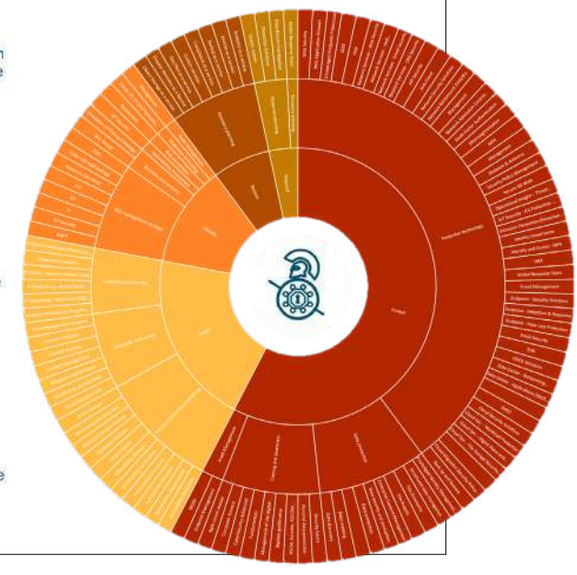
Competenza - Disponiamo di un gruppo di analisti estremamente competenti e certificati in grado di studiare e suggerirvi le corrette tecnologie. Inoltre abbiamo predisposto un catalogo corsi con l'obiettivo di trasferire competenze e conoscenze che vanno da elementi prettamente tecnologici a corsi su processi e organizzazione aziendale orientati alla sicurezza. Infine, crediamo nella certificazione delle competenze e pertanto tutti i corsi, previo superamento di un esame, consentono di ottenere dei badges conformi al framework open badges 2.0. Exprivia ha anche sviluppato delle simulazioni (cyber-range) utilizzabili per valutare il grado di efficienza dell'azienda nel rispondere a un attacco.

Servizi

I servizi che Exprivia mette a disposizione sono disegnati sui controlli di sicurezza del National Institute for Standard and Technologies (NIST) e condividono i dati forniti dall'Osservatorio di CyberSecurity, si dividono in:

- **Identify** - Da attività consulenziali a Vulnerability e Penetration Test (VAPT), da simulazioni di campagne di malvertisement ad analisi e ricerca di dati eventualmente rubati ed esposti sul deep e dark web. Obiettivo è suggerire ai clienti processi e controlli per ridurre il rischio complessivo ottimizzando gli investimenti.
- **Protect** - Implementazione e gestione dei controlli che si focalizzano sulla protezione da eventuali incidenti, segmentazione, micro-segmentazione, gestione e governo identità e accessi, gestione delle identità privilegiate, sicurezza statica (SAST) e dinamica delle applicazioni (DASD), sicurezza, offuscamento e mascheramento dei dati a riposo e in transito.
- **Detect** - Monitoring continuo utilizzando SIEM e strumenti di AI sofisticati in grado di identificare i sintomi di un attacco prima che inizi.
- **Response** - Un incidente non dovrebbe mai accadere, ma se accade è meglio affidarsi alle mani di esperti che ne possano limitare e talvolta azzerare i danni. Exprivia è dotata di un team che può essere ingaggiato per rispondere a un incidente (Global Response Team).
- **Restore** - Ripristinare un servizio dopo un attacco non è la stessa cosa che ripristinare il servizio causato da agenti atmosferici sfavorevoli. Il GRT può essere utilizzato non sono per rispondere a un attacco, ma ripristinare il servizio.

Per tutti i servizi Exprivia è in grado di utilizzare il **modello di delivery** più adatto, gestendo tecnologie e processi presso i suoi clienti ma anche dalle proprie sedi.



Conoscenza delle Industrie

La CyberSecurity ha dei concetti generali, ma necessita di conoscenze molto specifiche sulle architetture e i processi utilizzati nell'industria. Exprivia ha sviluppato gran parte del suo successo sulla conoscenza di processi e architetture industriali, oggi questa conoscenza è a disposizione dei servizi di CyberSecurity.

exprivia

future. perfect. simple.

COVID-19 disegna nuovi scenari nella CyberSecurity

Ottimizzare gli investimenti per ridurre il rischio complessivo

Nuovi e più ampi scenari derivanti dagli impatti dell'epidemia COVID-19 impongono alle organizzazioni l'adozione immediata di rinnovati paradigmi operativi che evitino l'immobilizzazione: Exprivia affianca i propri clienti in questa sfida.

Le esigenze urgenti

- Abilitazione allo Smart Working di tutto il personale
- Protezione massima delle attività in Smart Working
- Gestione continuativa di sistemi aziendali remotizzata
- Revisione delle tecniche e strategie di controllo e monitoraggio delle attività, sia interne che esterne all'azienda

La risposta Exprivia

Consulenza – Servizi – Prodotti

Exprivia supporta i propri clienti con 6 soluzioni focalizzate e modulari a protezione delle attività in Smart & Safe Working.

exprivia

future. perfect. simple.

L'offerta modulare

Risk Exposure Calculator
Tool analitico a supporto delle fasi iniziali di assessment per clienti anche non ancora strutturati sul tema della Cybersecurity. Permette una rapida valutazione sull'esposizione dell'azienda verso le minacce più importanti.

Endpoint Threat Detection & Response Services
Database dinamico di Cybereason a grafi, centralizzato in memoria, che si evolve continuamente man mano che vengono raccolti nuovi dati. La tecnologia Deep Graph mette costantemente in relazione elementi tra gli endpoint di un'organizzazione, monitora milioni di relazioni tra punti dati ogni secondo, consente di aggregare automaticamente elementi interconnessi di un attacco e individuare attività sospette che altrimenti non sarebbero identificate.

Dynamic Microsegmentation Network Protection
Innovativa soluzione di Micro-segmentazione Dinamica con la quale diventa possibile e facile isolare le comunicazioni fra i diversi attori e componenti, definendo regole a livello logico e operativo. Si tratta dell'unica piattaforma di sicurezza convergente che copre completamente tutte le aree critiche per proteggere il traffico est-ovest: visibilità, micro-segmentazione, rilevamento delle violazioni, analisi automatica e risposta.

Endpoint Patch Management
Strumento che permette di smistare patch su endpoint distribuiti e virtuali utilizzando diversi sistemi operativi indipendentemente dalla posizione, dal tipo di connessione o dallo stato. Si tratta di una soluzione scalabile e facile per la gestione delle patch, la conformità, il ciclo di vita ed Inventory Management. Migliora la sicurezza e semplifica la gestione degli endpoint anche remoti.

Unmanaged/Managed Endpoint Protection
SentryBay Armored Client e Browser permettono di avere protezione anche se l'operatore lavora da sistemi privati/personali non gestibili dall'azienda creando un "area sicura" all'interno del dispositivo, protetta da malware eventualmente già presente sul sistema. Inoltre, incrementano il livello di sicurezza su apparati di proprietà dell'azienda o di fornitori esterni, rafforzando soluzioni di VDI, tool di remotizzazione e applicazioni SaaS.

Privileged Account Discovery/Assessment
CyberArk DNA (Discovery aNd Audit) è in grado di effettuare la scansione automatica di server Windows e *nix per trovare tutte le utenze con privilegi presenti, identificando problemi di compliance e vulnerabilità. Il rapporto, in formato Microsoft Excel comprende:

- censimento di tutte le utenze presenti sulle macchine Unix e Windows (locali o di dominio);
- individuazione di chiavi SSH distribuite sulle macchine, incluse chiavi orfane;
- disegno di mappe di vulnerabilità pass-the-hash per Windows.

Partner selezionati per questa offerta:

- CyberArk
- Cybereason
- Guardicore
- HCL
- Sentry Bay

www.exprivia.it

exprivia

future. perfect. simple.

Threat calculator: proteggersi, al meglio

CyberSecurity

Conosci i tuoi punti deboli? Sai come proteggerti?

Valutariamo il tuo attuale livello di protezione e ti proponiamo la soluzione più efficace ed efficiente in termini di costi e livelli di rischio.

Mappiamo i rischi e le vulnerabilità del tuo sistema informatico in via preliminare in modo accurato e sistematico.
Le informazioni raccolte sono mirate alla elaborazione di una strategia utile a limitare la tua esposizione ad ogni singola minaccia informatica.

I punti di forza di forza del nostro approccio

- Poca invasività
- Trasparenza
- Coinvolgimento del cliente
- Proposta personalizzata
- Ottimizzazione dei costi
- Completezza

exprivia

future. perfect. simple.

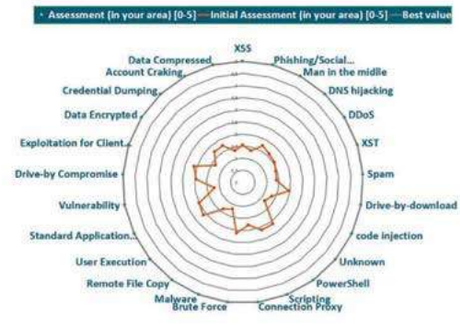
La nostra offerta

- Definizione dei potenziali attaccanti
- Conoscenza del loro comportamento
- Profilazione delle misure attualmente utilizzate
- Proposta ad-hoc per ottenere massima protezione

Il nostro approccio

- Analisi degli attacchi subiti in passato
- Verifica dei controlli di sicurezza implementati
- Questionario di valutazione delle misure di sicurezza attualmente osservate
- A profilazione completata ti mostriamo la tua situazione attuale mediante l'utilizzo di grafici esaustivi e chiari
- Proposta concreta sulle migliorie a maggiore impatto in termini di sicurezza

Il **Threat Exposure Calculator** è un tool analitico in grado di fornire in poche ore una valutazione sulla esposizione della azienda agli attacchi informatici.
Questo strumento permette di ottenere un quadro analitico globale relativo alla copertura di sicurezza dell'azienda, analizzando numerose tipologie di attacco e fornendo un'immagine efficace del proprio stato e suggerimenti sulle misure di mitigazione dei rischi da intraprendere.



Lo strumento consolida informazioni che vengono fornite dalla azienda sulle attività (tramite questionari o discussione telematica con un nostro analista) e sui controlli di sicurezza attivi; integrando anche informazioni raccolte interrogando fonti aperte e strumenti di Threat Intelligence.
Una volta completata la valutazione, e' possibile usare lo strumento per effettuare simulazioni e osservare in che modo il rischio possa essere mitigato eseguendo attività o implementando servizi.

exprivia

future. perfect. simple.

Threat Awareness Range: simuliamo scenari di attacco per definire strategie di contrasto

CyberSecurity

E-TAR, Exprivia Threat Awareness Range, è un ambiente nel quale è possibile simulare scenari di attacco reali, che aiutano a valutare le vulnerabilità e le capacità di difesa di un'entità e delle sue componenti e quindi a definire nuove ed efficaci strategie di contrasto alle minacce.

Il framework fornisce un servizio che permette, attraverso la simulazione di scenari di attacco reali, di individuare comportamenti critici legati al personale di un'entità. La simulazione vedrà come protagonisti i principali attori caratterizzanti l'ambiente in cui l'entità opera, che interagiranno in tempo reale e le cui scelte influenzeranno l'evoluzione di ogni singolo scenario di attacco.

Al termine di ogni scenario presentato verranno segnalate e analizzate le best practice da utilizzare in ogni singola situazione affrontata.

Exprivia ritiene questa soluzione fondamentale per fornire un miglioramento complessivo della qualità di risposta a incidenti di sicurezza.

exprivia

future. perfect. simple.

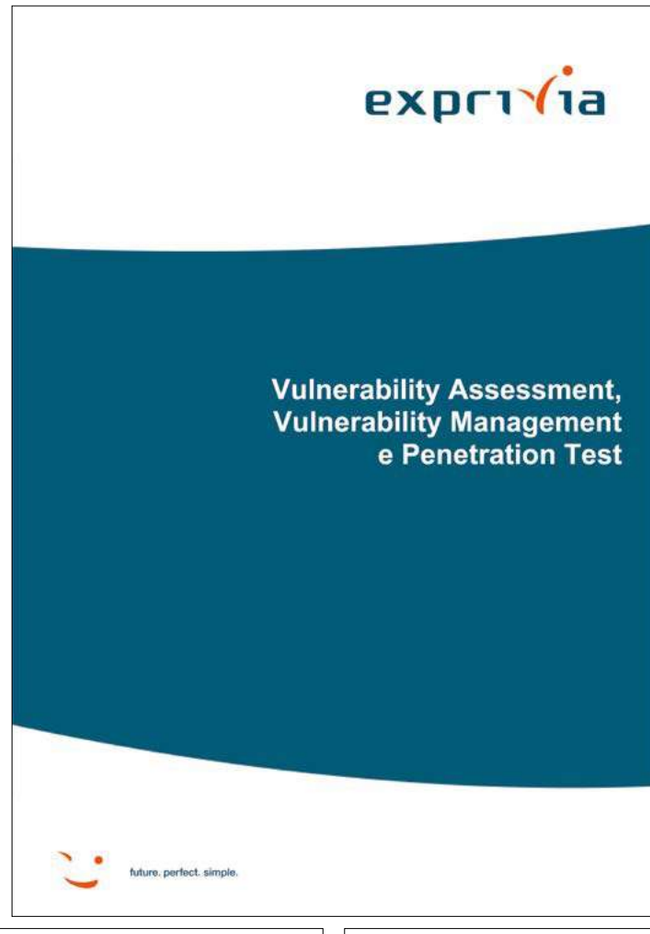
Punti di forza

- Interazione diretta con il personale dell'entità
- Presentazione di scenari complessi attraverso una soluzione user friendly e interattiva
- Continuo aggiornamento delle minacce
- Customizzazione degli scenari di attacco in relazione al dominio applicativo dell'entità interessata
- Controllo sulla simulazione mediante un'apposita dashboard
- Disponibilità in cloud

Il nostro approccio

Sessioni di training con analisi dei risultati derivanti dai report della simulazione e formazione in aula mirata allo sviluppo della consapevolezza sulla CyberSecurity.

www.exprivia.it



Vulnerability Assessment

Il **Vulnerability Assessment (VA)** fa riferimento all'analisi di sicurezza rivolta ad **individuare tutte le eventuali vulnerabilità** dei sistemi e delle applicazioni di una rete, attraverso una identificazione e valutazione dei possibili danni che l'attaccante potrebbe causare all'attività.
L'attività di Vulnerability Assessment può essere eseguita sia dall'interno che dall'esterno della rete aziendale consentendo di simulare diversi scenari che potrebbero verificarsi in un'azienda. Questo fornisce un report finale contenente le vulnerabilità che se risolte potrebbero garantire una sicurezza maggiore e un sistema più sicuro. Il Vulnerability Assessment deve essere garantito, in modo periodico, in presenza di dati sensibili, soprattutto dopo l'introduzione del GDPR.

A seguito del Vulnerability Assessment viene consegnato un report che descrive le vulnerabilità identificate seguite da eventuali soluzioni.

Servizi offerti

I servizi di Vulnerability Assessment che offriamo sono:

- **Scansioni relative al Networking e quindi ai dispositivi di rete:** eseguiamo scansioni di tutta la rete individuando: porte aperte, host attivi, versione del sistema operativo, versioni di web server e analisi dei pacchetti di rete.
- **Scansioni delle Reti Wireless:** realizziamo scansioni di tutta la rete Wireless con l'obiettivo di individuare delle vulnerabilità e password deboli.
- **Scansioni relative alle Web Application:** eseguiamo scansioni di un'intera Web Application individuando eventuali vulnerabilità partendo da un singolo IP/URL. Abbiamo tool che individuano la presenza di script vulnerabili all'interno della Web Application. Inoltre, testeremo le vulnerabilità già note per ottenere eventuali riscontri. Individuiamo i difetti che permettono di effettuare le SQL injection, così da evitare di perdere il controllo dei server DBMS. Infine, tutte le vulnerabilità trovate verranno elencato in base alla criticità.
- **Scansioni relative IoT:** constatiamo la presenza di password deboli o di default dei dispositivi che potrebbero causare l'accesso alla rete da utenti non autorizzati. Verifichiamo la presenza di comunicazioni non crittografate, presenza di firmware non aggiornati e controllo dei protocolli utilizzati. Tutto questo al fine di evitare manomissioni e che i dispositivi vengano utilizzati senza autorizzazioni.
- **Application Security Testing:** effettuiamo analisi statica (SAST), dinamica (DAST) e ibrida (IAST) del codice con lo scopo di individuare vulnerabilità. Infine, testeremo le vulnerabilità conosciute per ottenere riscontri.
- **Scansioni Utenze Privilegiate:** compiamo scansioni di sistemi Windows, Unix e Linux alla ricerca delle utenze privilegiate presenti. Sui sistemi Unix/Linux scansioniamo anche le chiavi SSH presenti nei repository standard. Forniremo quindi correlazioni sugli accessi avvenuti fra i server, in funzione della prevenzione di attacchi di tipo Pass-the-has.

Vulnerability Management

Il Vulnerability Management (VM) è una pratica ciclica e completamente automatizzata mirata a identificare, classificare, dare priorità, rimediare e mitigare le vulnerabilità.

Le vulnerabilità possono essere individuate tramite con uno scanner di vulnerabilità, il quale analizza un sistema alla ricerca di vulnerabilità note, come porte aperte, configurazioni software non sicure e suscettibilità alle infezioni da qualsi tipo di malware.

Questa attività ciclica garantisce un continuo controllo sul sistema in maniera che una vulnerabilità, una volta risolta, non possa ripresentarsi nuovamente.

Servizi offerti

Monitoraggio e controllo: vengono adottate tecniche che consentono di identificare e risolvere in pochi minuti i problemi di tutti gli endpoint: fissi, portatili, fisici e virtuali. Utilizziamo tool che aiutano i team della sicurezza a individuare e stabilire priorità delle minacce in modo accurato in tutta l'azienda e offrono insight intelligenti che consentono ai team di rispondere rapidamente per ridurre l'impatto degli incidenti.

Inoltre, accorpiamo i dati degli eventi di log provenienti da migliaia di dispositivi, endpoint e applicazioni distribuiti in tutta la rete, con il fine di stabilire una correlazione tra tutte le varie informazioni e di raggruppare gli eventi correlati in singoli avvisi al fine di accelerare l'analisi e la correzione degli incidenti.

- Penetration Test delle applicazioni Web;
- Attacchi lato client;
- Utilizzo di exploits sulla base delle informazioni fornite sui sistemi;
- Pentration test su traffico di rete;
- Uso di malware controllati (backdoor, reverse shell).

Serivizi offerti

I servizi di Penatration Test che offriamo sono:

- Penetration test su Web Application: effettuiamo test su Web Application individuando le vulnerabilità presenti. Possiamo introdurci nei sistemi utilizzando porte aperte, configurazione errate del sistema o sfruttando vulneabilità dovute a vecchie versioni di alcuni software. Abbiamo tool che ci permettono di effettuare anche penetrazioni manuali.
- Utilizza exploits per effettuare pen test su Windows, linux e Mac OS X: adottiamo tecniche che utilizzano exploit per sfruttare delle vulnerabilità conosciute ed entrare nei sistemi e recuperare dati sensibili senza autorizzazione.
- Pentration test su traffico di rete: adottiamo tecniche che permettono di intercettare il traffico di rete recuperando i dati sensibili che viaggiano non crittografati. Utilizziamo tool che effettuano sniffing di rete. Abbiamo a disposizone una suite completa per effettuare attacchi Man In The Middle.
- Penetration test sulle password: rendiamo più sicure le password: lo facciamo attraverso cracker molto veloci che effettuano attacchi di Brute Force basati su word list con lo scopo di individuare le password deboli cosi da sostituirle.
- Prestazione di malvertisement: è strutturato in modo tale da generare ed inviare ad una lista di utenti, una mail fake ben strutturata contente un link, con lo scopo di identificare tutti gli utenti che non controllano il mittente della mail e in modo del tutto naturale cliccano sul link. Il link punta ad un web-server che mappa l'utente che ha effettuato questo tipo di operazione.

Penetration Test

I Penetration Test sono indispensabili per valutare la sicurezza di un sistema informatico, validando e verificando l'efficacia dei controlli di sicurezza informatica.

In pratica si tratta di una vera e propria simulazione di attacco hacker che ha come obiettivo un perimetro limitato del sistema. Questi tipi di test vengono di solito eseguiti mediante tecnologie manuali o automatizzate con l'obiettivo di compromettere volutamente i sistemi.

Si eseguono questi test solo dopo aver ottenuto l'autorizzazione dall'obiettivo. A seguito del Penetration Test viene consegnato un report che descrive le vulnerabilità identificate e le tecniche utilizate per violare il sistema. L'ultimo passaggio è la correzione delle vulnerabilità individuate.

Abbiamo la possibilita di effettuare due tipi di Penetration Test : *Black Box e White Box.*

Black Box

Un test di attacco Black Box non si hanno informazioni riguardo l'infrastruttura IT su cui effettuare i test. I nostri tester agiscono immedesimandosi nei panni di un vero cracker, quindi per identificare le vulnerabilità verrano effettuati veri attacchi. Il nostro servizio analizza la struttura e quindi la sicurezza dei vostri sistemi informativi.

L'obiettivo della tecnica di Black Box è quello di analizzare tutta la sicurezza dei sistemi utilizzando varie tecniche come attacchi ad hoc o utilizzare tecniche di **ingegneria sociale** per individuare punti deboli. Eseguiremo test sui sistemi **IT**, sul vostro personale e sulla sicurezza fisica (backup).

Il Black Box Testing include tutti o la maggior parte dei nostri servizi :

- Penetration Test delle applicazioni Web;
- Uso dell'ingegneria sociale;
- Attacchi lato client;
- Uso di malware controllati (backdoor, reverse shell);
- Penetration Test sulle password.

In breve, nella tecnica Black Box non ci verrà offerta **nessuna informazione** sull'infrastruttura. Il cliente ci fornirà qualche indirizzo o solo il nome della società. Questo servizio è di natura adattiva e viene sempre fornito attraverso un team di professionisti, con competenze diverse in tutti i domini di sicurezza. I nostri professionisti sono certificati e continuamente aggiornati sulle dinamiche del campo della sicurezza. Inoltre, si occupano in prima persona di Threat Intelligence per essere sempre aggiornati rispetto i comportamenti dei nuovi malware e delle più recenti vulnerabilità.

White Box

In un test di attacco White Box i tester avranno **ricevuto informazioni** approfondite sui vari target e sull'intera infrastruttura. Questo tipo di test prevede una simulazione di scenari.

Alcune informazioni fornite al tester possono essere: documentazione, architettura, codice sorgente o password d'accesso ai sistemi. Questo test garantisce una copertura maggiore rispetto alle tipologie di attacchi differenti che potrebbero non essere notati nei test Black Box.

Con questo test sarà possibile guadagnare del tempo, in quanto non servirà effettuare la fase di ricognizione come nel Black Box dato che tutte le informazioni ci verrano fornite dal cliente.
Nei test di White Box forniamo:

- Valutazioni di vulnerabilità;

exprivia

Exprivia CyberSecurity Academy

future. perfect. simple.

exprivia

Il mondo della CyberSecurity è affascinante, ma necessita di forti specializzazioni. Con il fine di ridurre il gap tra coloro che si avvicinano al mondo del lavoro per la prima volta e l'enorme domanda presente sul mercato, Exprivia ha strutturato Exprivia CyberSecurity Academy.

I candidati sono studenti, laureati e non, con una forte passione per la CyberSecurity.

L'Academy è aperta anche a studenti che non hanno completato il percorso universitario. In questo caso Exprivia supporterà il candidato nella stesura della tesi di laurea.

Exprivia CyberSecurity Academy è un percorso formativo dedicato ai professionisti che vogliono trasformare la loro passione per la CyberSecurity in lavoro.

Percorso formativo e aree di specializzazione

La CyberSecurity è una disciplina in cui sono necessarie diverse specializzazioni che possono suggerire lavori di tipo diverso, dalla gestione dei sistemi di sicurezza all'analisi degli incidenti, da attività di consulenza su gestione dei rischi a analisi forense, dall'erogazione del servizio alla vendita e pre-vendita. Il nostro primo obiettivo è pertanto quello di comprendere le attitudini e i desideri suggerendo la specializzazione che meglio si adatta alle caratteristiche del candidato.

In funzione della specializzazione selezionata, l'obiettivo dell'Academy è quello di sviluppare il talento e migliorare le competenze dei partecipanti al programma fornendo loro:

1. una solida preparazione di base nel campo della CyberSecurity;
2. affiancamento a specialisti esperti della materia;
3. certificazioni sugli strumenti più utilizzati nel settore.

L'Academy prevede un percorso formativo di circa 8 mesi.

Nei primi cinque mesi i partecipanti acquisiranno nozioni di base sulla CyberSecurity.

In particolare, la formazione prevede lezioni su:

- **CyberSecurity Fundamentals** - Comprendere le diverse specializzazioni, definizioni, metodologie di attacco e attività, processi e organizzazione della sicurezza (*unattended* e *online/face-to-face learning*)
- **CyberSecurity Basics** – Individuare eventuali minacce, apprendere tecniche e metodologie per difendersi da malintenzionati, configurare correttamente il proprio dispositivo, classificare i diversi tipi di malware, phishing e vishing (*unattended*)
- **GDPR Basics** – La sicurezza richiede la conoscenza delle normative e regolamentazioni. Il GDPR è forse una delle più popolari (*unattended*)
- **Python Basics** – La CyberSecurity richiede conoscenze di programmazione, sistema operativo e rete. Il Phyton è un esempio di linguaggio di programmazione, ma saper programmare è necessario per chiunque. (*unattended*)
- **Internet of Things Fundamentals** – La CyberSecurity non può prescindere dal conoscere i rischi su IoT (*unattended*)
- **Network Basics** – Sviluppare le competenze necessarie per proteggere le reti e prevenire le intrusioni (*unattended*)
- **Introduzione a Powershell** – Insegnare le basi del linguaggio di scripting per l'amministrazione dei sistemi Windows (ora utilizzabile anche sui sistemi Linux) in rete aziendale. S'impareranno le basi del linguaggio, i metodi di concatenazione dei comandi, il controllo condizionale e le iterazioni, sino

future. perfect. simple. 2

exprivia

alla scrittura di script. Il corso introduce le basi di Powershell in modo pratico e con un'ottica rivolta ai sistemi. (*unattended*)

- **Operating System** – La CyberSecurity richiede conoscenze di programmazione, sistema operativo e rete. (*unattended*)
- **Application Security Basics** – Comprendere la sicurezza delle applicazioni, ovvero la disciplina di processi, strumenti e pratiche volte a proteggere le applicazioni dalle minacce lungo l'intero ciclo di vita dell'applicazione (*unattended*)
- **Public Speaking** – La CyberSecurity non ha un chiaro ed evidente ROI. Saper comunicare è importante tanto quanto erogare il servizio. (*unattended* o *online/face-to-face learning*)

È predisposta un'attività di laboratorio (opzionale):

- **Network Basics Lab** (online o face-to-face learning)
- **Application Security Basics Lab** (online o face-to-face learning)

Tutti i corsi rilasciano una certificazione della competenza acquisita tramite il framework open badge 2.0 previo superamento di un esame e attestato di partecipazione per i corsi erogati tramite la **piattaforma Udemy**.

A completamento di questa prima fase ai partecipanti verrà rilasciato il **badge di Exprivia CyberSecurity Academy Level I su framework open badge 2.0**.

Per accedere al livello due, sono previsti:

1. Badge di Exprivia CyberSecurity Academy Level I
2. Processo di selezione in funzione delle esigenze del mercato ed attitudini, competenze e aspettative dei candicati

Il percorso formativo, della durata di **due mesi**, relativo al Level II prevede una specializzazione su un'area specifica della CyberSecurity che meglio si adatta ai desideri ed attitudini del candidato.

La formazione nell'area identificata prevede l'affiancamento di una figura senior in azienda che con la sua esperienza potrà guidare al meglio l'acquisizione delle competenze.

Le aree di specializzazione attualmente identificate nel percorso sono:

- Identity&Access Management
- Network Security
- Security Operation Center (SOC)
- Vendita e Prevendita
- Programmazione e Application Security
- Endpoint Detection and Response (EDR)
- Vulnerability Assessment and Penetration Testing (VAPT)
- Incident Response e Analisi Forense

In funzione della specializzazione selezionata, ci saranno dei corsi e delle attività opportune.

Tutti i partecipanti a questa fase faranno il corso:

- **Service Management Foundation** - Nella CyberSecurity è necessaria una forte capacità di gestione e governance del servizio offerto.

future. perfect. simple. 3

exprivia

Tutti i corsi rilasciano una certificazione della competenza acquisita tramite il framework open badge 2.0 previo superamento di un esame e attestato di partecipazione per i corsi erogati tramite la **piattaforma Udemy**.

A completamento di questa seconda fase ai partecipanti verrà rilasciato il **badge di Exprivia CyberSecurity Academy Level II su framework open badge 2.0**.

Per accedere al livello tre, sono previsti:

1. Badge di Exprivia CyberSecurity Academy Level II

Durante questo periodo, che avrà la durata di **un mese**, i candidati potranno osservare progetti reali per potersi ulteriormente avvicinare al mondo del lavoro.

A completamento di questa terza fase ai partecipanti verrà rilasciato il **badge di Exprivia CyberSecurity Academy su framework open badge 2.0**, previa sottomissione ed accettazione di un package in cui il candidato presenterà un project work sviluppato durante l'ultima fase.

future. perfect. simple. 4

exprivia

future. perfect. simple.

Servizio di monitoraggio esterno

CyberSecurity

Il servizio di monitoraggio esterno Exprivia offre un'analisi approfondita e sistematica dei rischi e delle vulnerabilità esposte in rete.

È uno strumento che permette di tenere sotto controllo giornaliero tutti i servizi di un'organizzazione esposti in internet, notificandone immediatamente eventuali vulnerabilità.
Prevede l'invio di alert, in caso di attacchi o potenziali incidenti, e la stesura di report mensili sullo stato della propria sicurezza.
L'importanza del servizio di monitoraggio deriva dalla possibilità di difendersi in maniera efficace dal cyber crime attraverso la gestione dei dispositivi da remoto.
Non è necessaria alcuna competenza in materia cyber in quanto l'attività viene eseguita dall'esterno senza impatti operativi di alcun genere.
Il servizio è gestito da remoto da un team informatico altamente specializzato che si occupa del monitoraggio giornaliero e della produzione di report riassuntivi mensili. Il tutto a costi vantaggiosi.

exprivia

future. perfect. simple.

Negli ultimi anni il numero di **attacchi informatici**, **incidenti di sicurezza** e **violazioni privacy** è in netto aumento. I vettori di attacco sono tipicamente le attività di phishing e malware che rendono l'esposizione esterna delle organizzazioni al centro degli interessi dei cybercriminali.

Queste attività criminali hanno un obiettivo ben preciso, il **furto dei dati**. Il valore dei dati infatti, ha assunto negli ultimi anni un ruolo centrale nel panorama informatico ed i cyber criminali si sono sempre più attrezzati per rubarli o per organizzare estorsioni con conseguenze negative per le organizzazioni in termini pecuniari oltre che di immagine.

Il servizio di monitoraggio esterno Exprivia offre un'analisi approfondita dei rischi e delle vulnerabilità esposte in rete, svolta in modo accurato e sistematico.

Benefici del servizio

- Identifica in maniera approfondita le vulnerabilità della propria organizzazione e segnala le nuove vulnerabilità esterne che possono emergere ogni giorno.
- Permette di controllare i servizi web anche se implementati da fornitori terzi.
- Controlla ogni giorno se i propri sistemi esposti su internet abbiano nuove vulnerabilità e nel caso invia alert per segnalare l'esposizione e procedere con la bonifica.

Tipologia dei servizi

- **MCVE BASE**: pacchetto annuo che include il report mensile sullo stato della propria sicurezza, il monitoraggio giornaliero dell'organizzazione ed istruzioni di mitigazione.
- **MCVE ADVANCE**: pacchetto annuo che include il report mensile di sicurezza, il monitoraggio giornaliero, l'accesso alla piattaforma e un'analisi personalizzata sulla protezione dati.
- **MCVE FULL**: pacchetto annuo che include il report mensile di sicurezza, il monitoraggio giornaliero, il controllo rischio fornitori, l'analisi personalizzata sulla protezione dati e l'elaborazione di una strategia di sicurezza ad hoc.

www.exprivia.it

exprivia

future. perfect. simple.

Servizio di scansione delle vulnerabilità

CyberSecurity

Il servizio di scansione delle vulnerabilità Exprivia è un efficace strumento di prevenzione e controllo delle vulnerabilità esposte dai servizi di rete.

L'attività di Vulnerability Assessment Exprivia rappresenta un efficace strumento di prevenzione e controllo che permette di ottenere un'analisi completa delle vulnerabilità presenti e suggerisce le possibili soluzioni attraverso report dettagliati.
Viene realizzata un'approfondita analisi dei servizi connessi in rete come siti web, indirizzi e-mail, indirizzi IP, identificando in un determinato momento tutti i rischi informatici che potrebbero propagarsi e danneggiare l'intera infrastruttura.
Questo servizio ha un particolare vantaggio: non necessita di alcuna interazione tecnica in quanto effettuato dall'esterno, in breve tempo e senza impatti operativi di alcun genere. Non è necessaria, da parte del committente, alcuna specifica competenza tecnica poiché l'attività è eseguita completamente da remoto. Il report prodotto può essere utilizzato direttamente per indirizzare le azioni correttive. Il servizio è erogabile su sistemi operativi Windows, Linux, MacOS, Android, iOS. Il tutto a costi vantaggiosi.

exprivia

future. perfect. simple.

www.exprivia.it

Negli ultimi anni il numero degli attacchi informatici è in netto aumento. Tutte le organizzazioni, piccole e grandi, sono un potenziale obiettivo di azioni criminali. Il valore dei dati, infatti, ha assunto negli ultimi anni un ruolo sempre più fondamentale nel panorama informatico ed i cyber criminali si sono sempre più attrezzati per rubarli o per organizzare estorsioni.

Le informazioni rappresentano un piccolo tesoro da custodire. In caso di compromissione o furto di dati, si rischia di incorrere in pesanti sanzioni oltre che in ingenti danni di immagine.

L'esposizione di servizi delle organizzazioni verso la rete assume oggi un valore centrale negli interessi dei cybercriminali e nelle strategie di prima difesa, tuttavia, le competenze tecniche necessarie a realizzare e mantenere una corretta protezione sono in continua evoluzione e le diverse organizzazioni possono avere difficoltà a tenere il passo.

Tipologia dei servizi

- **SVE BASE**: il pacchetto include la scansione di 1 indirizzo IP, 1 dominio web e 1 dominio mail.
- **SVE EXTENDED**: il pacchetto include la scansione di 8 indirizzi IP, 2 domini web e 2 domini mail.
- **SVE ADVANCE**: il pacchetto include la scansione di 32 indirizzi IP, 4 domini web e 4 domini mail.
- **SVE ADVANCE PLUS**: il pacchetto include la scansione di 64 indirizzi IP, 10 domini web e 10 domini mail.

Benefici del servizio

- Identifica in maniera approfondita le vulnerabilità e i rischi presenti nell'interfaccia verso l'esterno della propria organizzazione.
- Riduce il rischio di attacchi informatici attraverso un controllo efficace di dispositivi, indirizzi mail e siti web connessi in rete.
- Effettua la scansione istantanea e fornisce all'utente i risultati, tramite un semplice ma completo report.

exprivia

future. perfect. simple.

CyberSecurity: la prevenzione ai confini della tecnologia

La Sanità, già minacciata dagli hacker, oggi affronta COVID-19.

L'aumento esponenziale registrato negli attacchi alla Sanità è dettato dalla criticità del servizio e dalla tipologia dei dati gestiti che rendono il settore estremamente appetibile a chi è interessato a trarne profitto illegalmente vendendo i record nel Dark Web o chiedendo denaro in cambio della promessa di ripristinare o non interropere il servizio stesso.

L'emergenza COVID-19 e il ruolo del Dark Web

L'emergenza COVID-19 e la necessità di doversi spesso affidare alla Telemedicina per diagnosi remote hanno reso i servizi forniti dalla Sanità ancora più critici.
Se sul Dark Web ieri si potevano trovare record di pazienti, oggi si possono trovare mascherine e medicamenti che suggeriscono come prevenire e curare il coronavirus.

exprivia

future. perfect. simple.

Valutazione del rischio e investimento

Se le minacce rappresentano una evidente criticità, non dissipare il budget dedicato a misure di CyberSecurity con scelte fatte sotto pressione e in emergenza risulta una necessità.
Importante è comprendere l'esposizione alle minacce prima di decidere quale misura adottare. Exprivia mette a disposizione dei suoi clienti un framework consolidato che studia la tipologia delle minacce e ne valuta il rischio associato in funzione della postura del cliente, dello stato del cliente e di ulteriori misure che sono già state adottate.

Quali sono le misure principali da adottare?

- **Migliorare la capacità di riconoscimento di un attacco:** questo servizio è fornito da un Security Operation Center (SOC) spesso non disponibile presso aziende sanitarie e ospedali. Exprivia offre servizi di monitoraggio espletati dai propri SOC, certificati ISO27001 e specializzati sulla Sanità.
- **Endpoint Detection e Response**: soluzioni in grado di identificare anomalie e bloccare eventuali intrusioni.
- **Microsegmentazione**: necessità di definire delle policies di accesso in funzione di tag assegnati a risorse e persone aventi ruoli e criticità diverse.
- **Unmanaged Endpoint Protection**: non sempre è possibile fornire e gestire direttamente gli apparati in uso agli utenti finali, ma è necessario permettere l'utilizzo di sistemi personali che potrebbero non essere adeguatamente protetti. Tuttavia è possibile identificare e fornire soluzioni tecnologiche che forniscano controlli essenziali senza la necessità di doverli gestire direttamente e senza assumerne il controllo
- **Migliorare la consapevolezza**
  - Bastano corsi di poche ore per ridurre l'incidenza del fattore umano in un incidente di sicurezza.
  - Simulare campagne di malvertisement e phishing in modo da poter identificare le aree di intervento.
  - Simulare tramite cyberrange specializzati sulla Sanità degli incidenti, al fine di verificare come gli attori coinvolti siano in grado di rispondere.

Generare valore, parlano di noi!

NETWORK DIGITAL 360

CYBERSECURITY360

Le sfide della cyber security per il 2020: i consigli per affrontarle con consapevolezza

Home > Soluzioni aziendali

Per affrontare le sfide continue della cyber security è necessaria maggiore consapevolezza dei rischi e della prevenzione. Ecco tutti i consigli per aver chiaro il quadro della situazione

29 Gen 2020

Domenico Raguseo
Head of CyberSecurity Exprivia

SECURENEWS

IL MAGAZINE DEDICATO A VIGILANZA & SICUREZZA

Cybercrime, Domenico Raguseo (Direttore Cybersecurity di Exprivia): “Attacchi informatici in crescita durante la pandemia. Ecco su cosa investire per essere meno vulnerabili”

GIORNALE BOLOGNA

Dicembre 17, 2020

Cyberchallenge, gara tra under 23 per formare hacker 'etici'

L'università degli studi di Verona, del Politecnico di Milano e dell'Università di Pisa hanno vinto la CyberChallenge.IT, una competizione legata al mondo della cybersecurity che ha coinvolto 560 allievi, tra i 16 e i 23 anni, da gennaio a maggio. I giovani hacker 'etici' hanno perfezionato le loro competenze nell'ambito della sicurezza informatica, i corsi si sono concentrati su aspetti come la crittografia, la sicurezza delle reti e delle infrastrutture hardware e software.

sky tg24 | I NUMERI DELLA PANDEMIA | REPORTAGE UCRAINA | DIARI AFGHANI | SANREMO | SPETTACOLO

TECNOLOGIA | News | Approfondimenti | Software App | Telecomunicazioni | Internet | Now | Drive Club

Cyberchallenge, una gara tra under 23 per formare hacker consapevoli

17 dic 2020 - 14:43

La competizione ha coinvolto 560 allievi, tra i 16 e i 23 anni, da gennaio a maggio. I giovani hacker 'etici' hanno potuto perfezionare le loro competenze nell'ambito della sicurezza informatica

L'università degli studi di Verona, del Politecnico di Milano e dell'Università di Pisa hanno vinto la CyberChallenge.IT, una competizione legata al mondo della cybersecurity che ha coinvolto 560 allievi, tra i 16 e i 23 anni, da gennaio a maggio.

ANSA Software&App

Fai la ricerca | Vai al Meteo | ABBONATI | Accedi o Registrati

Cronaca | Politica | Economia | Regioni + | Mondo | Cultura | Tecnologia | Sport | FOTO | VIDEO | Tutte le sezioni +

ANSA.it › Tecnologia › Software & App › Cyberchallenge, gara tra under 23 per formare hacker 'etici'

Cyberchallenge, gara tra under 23 per formare hacker 'etici'

Sul podio Università Verona, Pisa e Politecnico di Milano

Redazione ANSA

ROMA

17 dicembre 2020
12:56
NEWS

L'università degli studi di Verona, del Politecnico di Milano e dell'Università di Pisa hanno vinto la CyberChallenge.IT, una competizione legata al mondo della cybersecurity che ha coinvolto 560 allievi, tra i 16 e i 23 anni, da gennaio a maggio.

UNIPINEWS

Università di Pisa

UNIPINEWS | EVENTI | FOTO | VIDEO | RASSEGNA STAMPA | ENGLISH NEWS

CyberChallenge.IT: premiata l'Università di Pisa, prima classificata nella sfida tra gli hacker etici italiani

Il team dell'Ateneo ha vinto la competizione organizzata dal Laboratorio Nazionale Cybersecurity del Cini

Durante una cerimonia online che ha registrato una partecipazione record nella storia del Laboratorio nazionale di cybersecurity, il consigliere scientifico del ministro dell'Università e della ricerca, Nicola Mazzocca, ha premiato i vincitori di **CyberChallenge.IT**, il programma italiano di formazione per i giovani talenti della **sicurezza informatica**, organizzato dal **Laboratorio Nazionale Cybersecurity** del **Cini (Consorzio Interuniversitario Nazionale per l'Informatica)**. Giunta alla **quarta edizione**, la gara costituisce l'evento finale del corso di formazione e sviluppo di competenze specialistiche legate al mondo della cybersecurity che ha coinvolto 560 allievi, tra i 16 e i 23 anni, da gennaio a maggio.

enigma defense

Home | About Us | Mission | Our Services | News | Policy

info@enigmadefense.it
+39 06 8881 6605

All Posts | Cybersecurity | Compliance & Regulation | data breach | Accedi / Iscriviti

admin · 9 dic 2020 · Tempo di lettura: 8 min

Campari, attacco hacker con furto dati: perché sta capitando a tante aziende e come difendersi

Anche Campari colpita dalla tecnica del doppio attacco, due terabyte di dati trafugati e la minaccia di pubblicarli se l'azienda non pagherà 15 milioni di dollari. Vediamo perché c'è un boom del fenomeno (Geox, Luxottica, Enel…) e che deve fare un'azienda per difendersi.

StartupItalia

L'intervista a Matteo Flora, Partner 42 Law Firm.
I rischi per aziende e cittadini

ALESSANDRO DI STEFANO 10 dic 2020

NETWORK DIGITAL 360

CYBERSECURITY360 Cybersecurity Nazionale Malware e attacchi Norme e adeguamenti Soluzioni aziendali

Cyber security, i crimini aumentano in linea con la curva epidemica: i consigli per difendersi

Home > Malware e attacchi hacker

Non è un quadro molto confortante quello che riguarda lo stato della sicurezza informatica in Italia, in un anno in cui il paese è sotto scacco della pandemia da Covid-19 mentre in ambito cyber security si assiste ad un aumento dei crimini in linea con la curva pandemica. Ecco i numeri e alcuni utili consigli per difendersi

09 Dic 2020

G **Rosita Galiandro**
Responsabile dell'Osservatorio di CyberSecurity di Exprivia

NETWORK DIGITAL 360

MENU Agenda Digitale Cittadinanza digitale Sicurezza Informatica Sanità digitale Industry 4.0 Infrastrutture digitali

SOVRANITÀ DIGITALE

Mercato europeo della cyber security, siamo in ritardo: sfide e opportunità per le imprese

Home > Sicurezza Digitale

In Europa manca una strategia per rendere competitivo sul mercato globale l'ecosistema di aziende specializzate in cyber security: eppure, è urgente sviluppare una visione in questa direzione

07 Dic 2020

Danilo D'Elia

Senior Policy Manager, European Cyber Security Organisation

Cybersecurity Trends

NEWS ARTICOLI VIDEO INTERVISTE FOR BEGINNERS FOR EXPERTS RUBRICHE SFOGLIA LA RIVISTA ABOUT US

Rapporto Clusit 2020 sulla Sicurezza ICT in Italia

Rapporto Clusit 2020 sulla sicurezza ICT in Italia

Presentata la nuova edizione del Rapporto Clusit 2020 sulla sicurezza cyber. Secondo l'Associazione Italiana per la Sicurezza Informatica la pandemia spinge il cybercrime.

Nei primi sei mesi dell'anno persiste il trend di crescita degli attacchi gravi (+7%): il 14% è a tema Covid-19. Registrato un aumento in Europa; malware, phishing e social engineering le tecniche più utilizzate. +85% gli attacchi alle infrastrutture critiche, +63% quelli al settore della ricerca.

NETWORK DIGITAL 360

CYBERSECURITY360 | Cybersecurity Nazionale | Malware e attacchi | Norme e adeguamenti | Soluzioni aziendali

Cyber security, tra percezione e consapevolezza: un gap da colmare soprattutto nel Sud Italia

Il processo di digitalizzazione corre veloce e tutti ne siamo consapevoli. Dobbiamo fare in modo, però, che questa consapevolezza non lasci indietro la presa di coscienza dei rischi relativi alla cyber security. Ecco le soluzioni per colmare questo gap, soprattutto nel Sud Italia

30 Mar 2020

Domenico Raguseo
Head of CyberSecurity Exprivia

ANSA.it Speciali | Fai la ricerca | Vai al Meteo | ABBONATI | Accedi o Registrati

Cronaca | Politica | Economia | Regioni + | Mondo | Cultura | Tecnologia | Sport | FOTO | VIDEO | Tutte le sezioni +

SPECIALI Ambiente • ANSA2030 • ANSA ViaggiArt • Eccellenze • Expo Dubai • Industry 4.0 • Legalità • Lifestyle • Mare • Motori • Salute • Scienza • Terra&Gusto

ANSA.it › Aziende ed Emergenza Covid19 › Exprivia offre consulenza cyber security

Exprivia offre consulenza cyber security

Aderisce a 'Solidarietà digitale' del ministero Innovazione

Redazione ANSA BARI 07 Aprile 2020 17:54

Scrivi alla redazione | Stampa

(ANSA) - BARI, 7 APR - La veloce adozione di nuove tecnologie durante questo periodo di emergenza epidemiologica espone ancora di più le imprese al rischio di attacchi informatici.

Reportec RIVISTE WHITEPAPER INCHIESTE PRIMO DIGIT ARTICOLI VIDEO NEWSLETTER

Gli esperti Exprivia in aiuto per la sicurezza aziendale

Con lo smart working si devono ridurre i rischi informatici. Exprivia ha aderito all'iniziativa 'Solidarietà digitale' con un servizio di consulenza gratuito

E' un dato di fatto che il ricorso a nuove tecnologie per il lavoro agile espone ancora più le imprese al rischio di attacchi informatici.

REDATTORE SOCIALE 2001 20 ANNI 2021

NEWSLETTER ABBONATI LOGIN CERCA

NOTIZIARIO LE STORIE I NUMERI RUBRICHE L'OPINIONE LIBRI BANCHE DATI SPECIALI CALENDARIO

In evidenza VOLONTARIATO ACCOGLIENZA MIGRANTI SCUOLA

Home / Notiziario / Coronavirus, consulenza gratis per...

7 aprile 2020 ore: 16:58
SOCIETÀ

RS

Coronavirus, consulenza gratis per valutare le minacce informatiche

INSURZINE MENU Cerca nel sito

CYBERSECURITY

Coronavirus, Exprivia: "Consulenza gratuita alle aziende per valutare le minacce informatiche"

Coronavirus, Exprivia: "Consulenza gratuita alle aziende per valutare le minacce informatiche". La veloce adozione di nuove tecnologie durante questo periodo di emergenza epidemiologica espone ancora di più le imprese al rischio di attacchi informatici. È per questo che Exprivia, con il supporto del proprio team specializzato in cybersecurity, ha deciso di offrire gratuitamente alle aziende [...]

08/4/2020 - by admin

INFORMAZIONE PER LA SICUREZZA
News web | webtv | magazine

Home » News » Cybersecurity

SICUREZZA DEI DATI, PRIVACY E PANDEMIA

di Redazione - 27 Maggio 2020

Come mettere in sicurezza il dato sensibile? È la domanda al centro dell'articolo che segue a cura di Domenico Raguseo, Head of CyberSecurity **Exprivia Italtel** e Docente presso l'**Università degli Studi di Bari**. Raguseo fa un'analisi della situazione attuale, degli eventi di **cybercrime** in relazione al COVID-19, ma anche di quelli che **con il COVID-19 nulla hanno a che fare e che sono altrettanto, e forse in prospettiva ancora più, rilevanti**.

Automazione news
Digital Mindset | Ricerca e sviluppo | Applicazioni | Tecnologia | Prodotti | Scenari | More ›
INDUSTRIA 4.0 | PROCESS AUTOMATION | FACTORY AUTOMATION
Home › Process Automation › Safety e Cybersecurity › Osservatorio Cybersecurity Exprivia: in pericolo i sistemi di videosorveglianza

Osservatorio Cybersecurity Exprivia: in pericolo i sistemi di videosorveglianza

nb 5 Agosto 2020

L'emergenza Covid-19 in Italia ha influito pesantemente sulla sicurezza informatica anche post emergenza. Stando a quanto risulta dal secondo rapporto sulle minacce informatiche nel 2020 in Italia elaborato dall'**Osservatorio sulla Cybersecurity di Exprivia, giugno è stato il mese in cui dall'inizio dell'anno si sono verificati la maggior parte di attacchi, incidenti e violazioni della privacy** a danno di aziende, privati e pubblica amministrazione.

WIRED
SCIENZA ECONOMIA CULTURA GADGET SECURITY DIRITTI IDEE VIDEO PODCAST

GABRIELE PORRO SECURITY 30.07.2020

I cyber-attacchi in Italia sono sempre di più

Secondo una ricerca di Exprivia negli ultimi tre mesi le minacce informatiche sono aumentate a dismisura, con un picco a giugno

In **Italia** gli attacchi informatici sono **aumentati di oltre il 250%** nel secondo trimestre rispetto ai primi tre mesi del 2020 facendo registrare un preoccupante **picco nel mese di giugno**.

A riportare i dati sulla situazione della sicurezza di rete in Italia è l'osservatorio cybersecurity di Exprivia, società italiana di informatica, che nel suo report ha evidenziato come l'**emergenza Covid-19** abbia influenzato pesantemente la **sicurezza informatica** in Italia. L'aumento dei lavoratori in smart working ha creato un campo fertile per il cybercrime.

NETWORK DIGITAL 360

Menù | InsuranceUp | Scenari | Opinioni | Business | Startup | Open-F@B | EconomyUp

I rischi della vita online, come aumentare la sicurezza

Home > Business

Con la pandemia la rivoluzione digitale ha raggiunto il suo più incredibile momento di accelerazione, sia in ambito lavorativo e business, che in ambito privato e personale. Questo ci espone tutti, aziende e persone fisiche, a maggiori rischi

24 Ago 2020

Barbara Bosco
Redattore

Qdpnews.it
QUOTIDIANO DEL PIAVE

Comuni | Al Microfono

Attacco hacker nei social di Luca Zaia: violati gli account whatsapp e instagram del Presidente della Regione

DI LUCA COLLATUZZO · GIOVEDÌ, 17 SETTEMBRE 2020 · 1 MINUTE READ

La denuncia del Governatore del Veneto è scattata quest'oggi, giovedì 17 settembre, sul proprio profilo Facebook: "**Sono stato vittima di hackeraggio su whatsapp e sul mio profilo Instagram**. Ho ripristinato i social e il numero telefonico, ma al momento non riesco a ricevere messaggi whatsapp. Conto di risolvere il problema al più presto".

SEZIONI | VIDEO | RUBRICHE | CONTRIBUTORS | INFO | key4biz | NEWSLETTER

HOME » CYBERSECURITY » CYBERCHALLENGE.IT, AL VIA LA FINALE DEGLI HACKER ETICI ITALIANI

FORMAZIONE

CyberChallenge.IT, al via la finale degli hacker etici italiani

di **Redazione Key4biz** | 1 Ottobre 2020, ore 15:00

Giunta alla quarta edizione, la gara, in programma oggi e domani, costituisce l'evento finale del corso di formazione e sviluppo di competenze specialistiche legate al mondo della cybersecurity che ha coinvolto 560 allievi, tra i 16 e i 23 anni, da gennaio a maggio.

deepblue

CONSULTING ¬ RESEARCH ¬ ABOUT ¬ NEWS BLOG CONTACT

16 OCT **CRIMINALI INFORMATICI ALL'ATTACCO DI PMI E MICROIMPRESE**

Posted at 11:00h in Blog by Vera Ferraiuolo

La rivoluzione digitale è in atto. I **processi produttivi e l'erogazione dei servizi sono sempre più basati su tecnologie digitali**. Con prospettive di sviluppo e mercato entusiasmanti, ma anche pericolosi effetti collaterali, come l'**aumento del rischio informatico**. Se le grandi compagnie sono più attente e dispongono di risorse da destinare alla sicurezza informatica, spesso le piccole, medie e micro imprese non sono preparate ad affrontare i pericoli cibernetici. E forse proprio per questo sono sempre più prese di mira dai cyber criminali. Secondo un **report del 2019** dell'istituto di ricerca Ponemon, infatti, **dal 2016 gli attacchi informatici verso le PMI sono aumentati globalmente di oltre il 20%**, procurando ogni anno danni economici per **oltre 2,2 milioni di dollari**. Negli ultimi anni, **più del 49% degli attacchi informatici** ha colpito piccole attività.

Allianz | Allianz Darta Saving

MONDO ALLIANZ DARTA FONDI INVESTIMENTO L'ESPERTO RISPONDE ATTUALITÀ STORIE NEWSLETTER CONTATTI

5 Ott 2020

Covid-19, cresce il digitale ma serve sicurezza: la Cyber Insurance per frenare il Cyber Risk

La necessità di coniugare le **misure anti Covid-19** – in particolare, la riduzione di contatti diretti – con l'esigenza di continuare a svolgere **attività lavorative e scolastiche** ha incrementato la **propensione all'uso del digitale**, dando impulso a un trend già in corso.

Posta Elettronica Rubrica Servizi on-line Scuole di Ateneo Dottorato International Cerca

UNIVERSITÀ DI CAMERINO

MY UNICAM

Futuro Studente Studente Laureato Personale

PRESS ROOM

Comunicati Stampa
Oggi in edicola
Cartella stampa
#ilfuturononcrolla
Manuale di Identità Visiva

Home / Winter school su "Blockchain technology and applications"

Winter school su "Blockchain technology and applications"

L'Università di Camerino organizza dal 14 al 18 dicembre 2020 la "International on line winter school on Blockchain technology and applications", per approfondire la nuova tecnologia blockchain con un focus particolare su Hyperledger Fabric.

L'interesse per la blockchain, un registro pubblico digitale distribuito su più nodi il cui contenuto è organizzato in blocchi fra loro legati tramite crittografia, è infatti recentemente tornato alla ribalta per le sue potenzialità per l'applicazione in altri settori rispetto a quello puramente finanziario, in particolar modo nell'ambito della tracciabilità e della certificazione della produzione.

NETWORK DIGITAL 360

RISK MANAGEMENT 360

Il Cybercrime può minacciare il settore sanitario

Home > Cybersecurity

Nella sanità vengono gestiti dati molti critici che riguardano i pazienti. Non si tratta solo di garantire le opportune cure, ma è necessario anche che i dati vengano protetti garantendone riservatezza e integrità, che siano carte di credito o cartelle cliniche, se i dati dei pazienti finissero nelle mani sbagliate le conseguenze sarebbero facilmente immaginabili

27 Ott 2020

Domenico Raguseo

WIRED SCIENZA ECONOMIA CULTURA GADGET SECURITY DIRITTI IDEE VIDEO PODCAST

RAFFAELE ANGIUS E LUCA ZORLONI ECONOMIA 17.10.2020

C'è un made in Italy della sicurezza informatica. E ora vuole crescere in Borsa

Sono ancora poche le aziende nazionali della cybersecurity, ma vogliono diventare grandi. In Borsa Tinexta e Cyberoo lanciano la sfida

Chi Siamo / Contatti / Avvertenze / E-books / Segnali di Borsa / PdB Trading System / Pubblicità / Mailing List / PdB TV

ProiezionidiBORSA
TESTATA GIORNALISTICA SPECIALIZZATA IN NEWS E SOLUZIONI

Aggiornato alle 15:44 di lunedì 07 febbraio 2022

FINANZA E MERCATI | DIRITTO E FISCO | RISPARMIO E FAMIGLIA | LAVORO E DIRITTI | LIFESTYLE

Cerca nel sito

Consigliati

HOME » RISPARMIO E FAMIGLIA » Sfruttare il coronavirus per sferrare l'attacco ai nostri dati personali

Risparmio e Famiglia | NICOLA SANTULLI - 17 NOVEMBRE 2020 - 13:18 | Condividi | Twitter | Facebook

Sfruttare il coronavirus per sferrare l'attacco ai nostri dati personali

I cybercriminali ne sanno una più del diavolo e quando il contesto storico è ballerino riescono a mettere a segno colpi sensazionali. Ebbene, questi malintenzionati hanno saputo sfruttare il coronavirus per sferrare l'attacco ai nostri dati personali. La metà degli attacchi a tema coronavirus sono stati fatto tramite phishing, social engineering e malware.

La rete informatica sotto assedio

HOME | EMERGENZA COVID-19 | PETROLIO | CRONACHE | SOCIETÀ | POLITICA | LAVORO E SALUTE | ALTRE

Gazzetta della Val d'Agri

Curiosità, Notizie dall'Italia e dal Mondo

Reati informatici in Italia: ecco i più comuni

Gianfranco Grieco | 897

Condividi

Il numero dei reati informatici durante questa pandemia è in forte crescita rispetto agli anni precedenti. Complice il lockdown e tutte le misure restrittive messe in atto, moltissime persone si sono ritrovate da un giorno all'altro a spostare tutte le proprie attività

PM | CATEGORIE | Cerca... | ISCRIVITI ALLA NEWSLETTER | ARCHIVIO NEWSLETTER | REDAZIONE | PUBBLICITÀ | CONTATTI

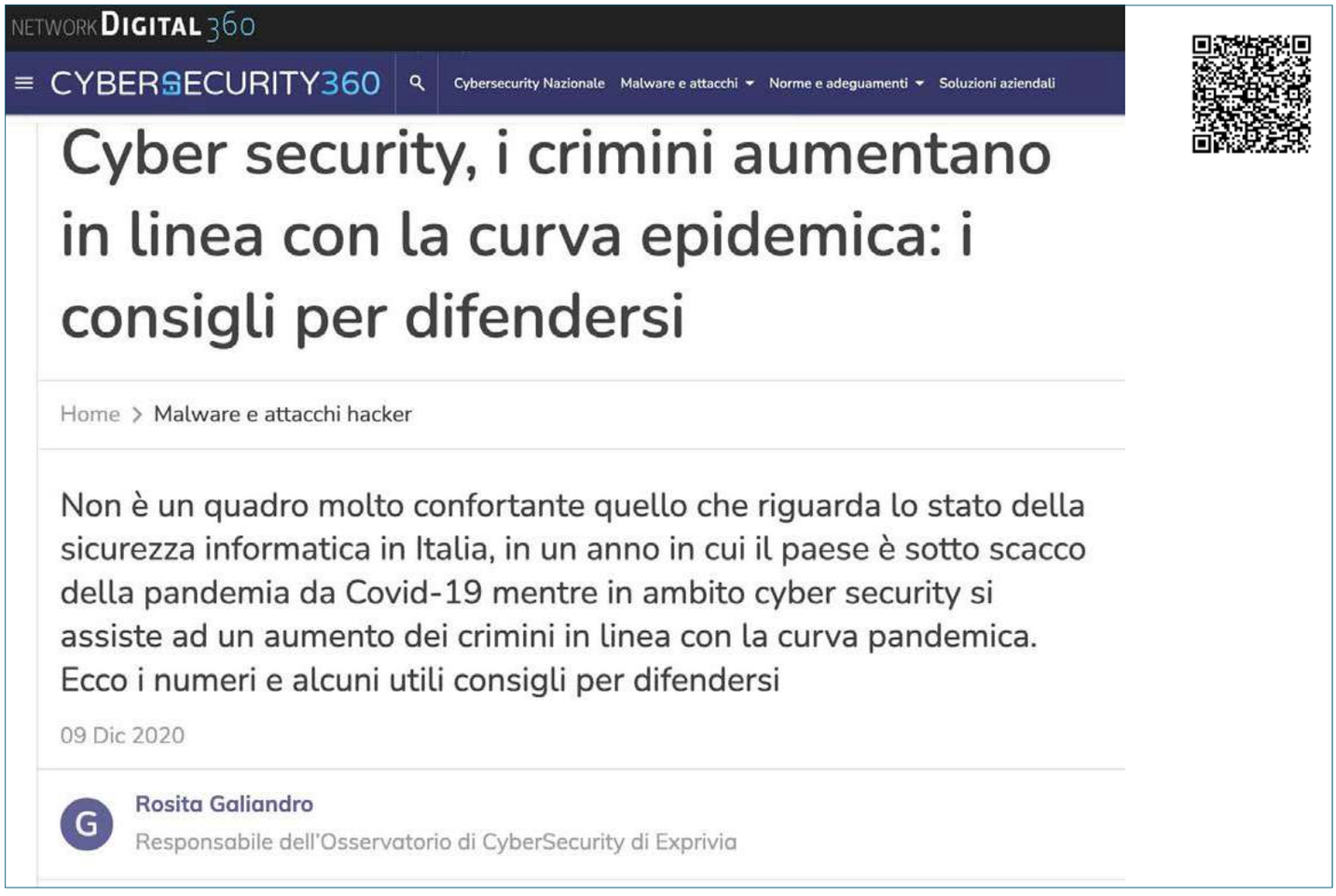
PAROLE di Management
QUOTIDIANO DI CULTURA D'IMPRESA
TESTATA GIORNALISTICA AUTORIZZATA

Lunedì 7 Febbraio 2022

Se Google è vulnerabile, chissà le PMI

SCRITTO DA GIORGIA PACINO IL 15 DICEMBRE 2020 PUBBLICATO IN SICUREZZA

Persino Big G si è fermato. Lunedì 14 dicembre 2020 i servizi di Google sono andati in down in diverse parti del mondo, causando decine di migliaia di segnalazioni. Soprattutto dall'Europa, per via del fuso orario, ma anche da Stati Uniti, Australia, Sudafrica e India.



NETWORK DIGITAL 360

CYBERSECURITY360 | Cybersecurity Nazionale | Malware e attacchi | Norme e adeguamenti | Soluzioni aziendali

Cyber security, i crimini aumentano in linea con la curva epidemica: i consigli per difendersi

Home > Malware e attacchi hacker

Non è un quadro molto confortante quello che riguarda lo stato della sicurezza informatica in Italia, in un anno in cui il paese è sotto scacco della pandemia da Covid-19 mentre in ambito cyber security si assiste ad un aumento dei crimini in linea con la curva pandemica. Ecco i numeri e alcuni utili consigli per difendersi

09 Dic 2020

Rosita Galiandro
Responsabile dell'Osservatorio di CyberSecurity di Exprivia

NETWORK DIGITAL 360

INTERNET 4.THINGS

Direttore Responsabile: **Maria Teresa Della Mura**

INDUSTRY 4.0 | SMART CITY | MOBILE WEARABLE | SMART BUILDING | SMART AGRIFOOD | SMART HEALTH

.sicurezza iot

SICUREZZA

Dispositivi connessi in rete e cybersecurity: i videogame possono essere un punto debole

Videogame e cybersecurity: se si sta utilizzando un computer o un dispositivo per entertainment, bisogna assicurarsi che lo stesso abbia tutti i controlli attivati, che il DNS sia opportunamente configurato, che la rete sia opportunamente protetta

di Domenico Raguseo, Exprivia

21 Dicembre 2020

CATEGORIE:
Sicurezza IOT

Uno degli effetti più evidenti della pandemia è che si passa più tempo a casa. A rendere più tollerabile il lockdown ci pensano, oltre che TV e Internet, anche tutte le soluzioni di intrattenimento, a partire dai **videogame**. Lavorare da remoto non ci rende tanto distanti dal mondo simulato e utilizzare in maniera intensiva il mondo

INFORMAZIONE PER LA SICUREZZA
News web | webtv | magazine

Cerca ...

NEWS » WEBTV » AZIENDE TECNOLOGIE RIVISTA EVENTI CONTATTI

Home » News » Cybersecurity

Crimini informatici: aumentano gli incidenti di sicurezza in Italia

di Redazione - 23 Dicembre 2021

Nel **Threat Intelligence Report 3Q 2021** dell'**Osservatorio Cybersecurity** di Exprivia emerge un **costante aumento degli incidenti informatici in Italia** che provocano danni a istituzioni, aziende e privati cittadini. Precisamente, tra luglio e settembre 2021 il Rapporto evidenzia 273 episodi di cui 166 attacchi, 93 incidenti di sicurezza e 14 violazioni privacy.

"Come suggeriscono i dati dell'Osservatorio di Exprivia – sottolinea Domenico Raguseo, Head of CyberSecurity Exprivia – è evidente un numero di incidenti di sicurezza in crescita, a fronte di una forbice tra attacchi informatici ed incidenti di sicurezza che si è andata a restringere ancora di più rispetto al 2Q 2021".

Infatti, nel 3Q 2021 è stato registrato il minor numero di attacchi da inizio anno, mentre il numero di incidenti di sicurezza (attacchi andati a buon fine) è stato il dato più alto rilevato. **Nonostante gli attacchi siano diminuiti, questi hanno causato un maggior numero di incidenti.** Ciò dovrebbe suggerire che gli attaccanti sono sempre più bravi.

NETWORK DIGITAL 360

CYBERSECURITY360

Cyber security, i crimini aumentano in linea con la curva epidemica: i consigli per difendersi

Home > Malware e attacchi hacker

Non è un quadro molto confortante quello che riguarda lo stato della sicurezza informatica in Italia, in un anno in cui il paese è sotto scacco della pandemia da Covid-19 mentre in ambito cyber security si assiste ad un aumento dei crimini in linea con la curva pandemica. Ecco i numeri e alcuni utili consigli per difendersi

09 Dic 2020

Rosita Galiandro
Responsabile dell'Osservatorio di CyberSecurity di Exprivia

NETWORK DIGITAL 360

CYBERSECURITY360

La cyber security nell'automotive: il ruolo dei Vehicle-SOC (V-SOC) per la mitigazione dei rischi

Home > Soluzioni aziendali

Nel mondo automotive componenti e sistemi connessi sono fondamentali per migliorare le capacità dei veicoli, ma introducono ulteriori vulnerabilità e punti di ingresso. Nella gestione del perimetro esteso su cui viaggiano i dati critici condivisi tra veicoli giocano un ruolo importante i Vehicle-SOC (V-SOC). Ecco perché

09 Dic 2021

Mario Direnzo
Responsabile sistemi informativi e Responsabile sviluppo nuovi prodotti software, Macnil

Domenico Raguseo
Head of CyberSecurity Exprivia

MarketScreener

BORSA | NOTIZIE | ANALISI | CONSIGLI | PORTAFOGLI | ELENCHI | MIGLIORI E PEGGIORI | SCREENERS

Home > Azioni > Italia > Borsa Italiana > Exprivia S.p.A. > Notizie > Riassunto XPR IT0001477402

EXPRIVIA S.P.A. (XPR)

Tempo reale stimato Cboe Europe - 15/02 15:53:23
2.035 EUR +1.24%

14/02 **EXPRIVIA S P A**: La Repubblica ed Bari - Grottaglie Droni a bassa quota, il progetto s... PU
03/02 **EXPRIVIA S P A**: Borsa Italiana - Il calendario 2022 degli eventi societari di Exprivia PU
03/02 **DATA MANAGER - PARKINSON**: un robot per la terapia dei pazienti a ritmo di danza ... PU

Riassunto | Quotazioni | Grafici | Notizie | Rating | Agenda | Società | Finanza | Consensus | Revisioni | Derivati

Riassunto | Tutte le notizie | Altre lingue | Comunicati stampa | Pubblicazioni ufficiali | Notizie del settore

Exprivia S p A : Women For Security - Sai riconoscere un email di phishing?

02-12-2021 | 18:11

30/11/2021

Argomento: Exprivia si parla di noi

Dati finanziari EUR

Fatturato 2021	175 M	Capitalizzazione	95,1 M
Risultato netto 2021	-	VS / Fatturato 2021	0,74x
Indebitamento netto 2021	34,0 M	VS / Fatturato 2022	0,65x
P/E ratio 2021	11,7x	N. di dipendenti	-
Rendimento 2021	-	Flottante	44,7%

» Più Dati finanziari

Grafico EXPRIVIA S.P.A.

Durata : Auto. Periodo : Giorno

NETWORK DIGITAL 360

CYBERSECURITY360

Ransomware e tecniche di elusione: evoluzione della minaccia e soluzioni preventive

Home > Malware e attacchi hacker > Ransomware

Sono oltre 80 milioni i campioni di ransomware identificati negli ultimi anni, suddivisi in 130 differenti "famiglie". Cifre che evidenziano quanto questo malware sia diffuso e quanto possa essere facile contrarlo non avendo adeguati sistemi di protezione. Analizziamone il comportamento per imparare a difenderci

15 Nov 2021

Antonio De Chirico
SOC Manager Exprivia

MarketScreener

BORSA | NOTIZIE | ANALISI | CONSIGLI | PORTAFOGLI | ELENCHI | MIGLIORI E PEGGIORI | SCREENERS

Riassunto | Quotazioni | Grafici | Notizie | Rating | Agenda | Società | Finanza | Consensus | Revisioni | Derivati

Riassunto | Tutte le notizie | Altre lingue | Comunicati stampa | Pubblicazioni ufficiali | Notizie del settore

Rai3 - Cybersecurity: in Puglia, il Security Operation Center monitora gli attacchi informatici.

30/11/2021 RAI 3

SICUREZZA IN RETE BUONGIORNO REGIONE PUGLIA

NETWORK DIGITAL 360

CYBERSECURITY360

Maze e Ransomware as a Service: sanità sotto minaccia della doppia e tripla estorsione

Home > Malware e attacchi hacker > Ransomware

Il ransomware è una forma di criminalità informatica sempre più dirompente anche perché l'aumento delle tattiche di pressione aumenta la probabilità di un profitto: ciò è ancor più vero nel settore sanitario. Ecco i motivi, i possibili impatti e le soluzioni di mitigazione del rischio

21 Giu 2021

P Antonio Pontrelli
Responsabile del SOC Exprivia

Attualissimo Tech

I SAY BLOG

NEWS | DONNA | SPETTACOLO | SCIENZA | TECH | SPORT | LAVORO | GOSSIP | LIFESTYLE | MUSICA

NEWS | SOCIAL NETWORK | MOBILE | PC | APPLE

Furti di dati e riscatti, la nuova vita degli attacchi digitali

Stando ai dati dell'ultimo Rapporto sulle minacce informatiche, gli attacchi sarebbero diminuiti ma la minore numerosità è corrisposta a un incremento del tasso degli attacchi riusciti.

di ***Redazione*** | 24 Novembre 2021 | 11:59

Secondo quanto affermano gli ultimi dati dell'osservatorio Exprivia sulla sicurezza informatica, nel corso del terzo trimestre 2021 sono aumentati in misura significativa gli **attacchi informatici tentati e riusciti**. A preoccupare non è, infatti, il solo numero degli attacchi digitali in termini assoluti (peraltro in lieve calo rispetto al trimestre precedente), quanto piuttosto il fatto che **gli attacchi siano stati sempre più sofisticati e aggressivi**, e dunque più difficili da

NETWORK DIGITAL 360

CYBERSECURITY360

Cyber crime e consapevolezza, importante investire in cultura della sicurezza: ecco perché

Home > Cultura cyber

La pandemia ha contribuito a velocizzare il processo di digitalizzazione: la conseguenza è una distribuzione sempre più uniforme del cyber crime su tutto il territorio italiano e questo ci ricorda che la mancanza di cultura di sicurezza è la vulnerabilità maggiormente sfruttata dagli attaccanti

29 Apr 2021

Domenico Raguseo
Head of CyberSecurity Exprivia

Puntoinformatico

Digital economy | Software | Sicurezza | Telecomunicazioni | Hardware | Pubblicità su PI

Impara basi cybersecurity e privacy online con questo corso

Volete apprendere più nozioni in ambito cybersecurity e privacy online? Questo corso disponibile su Udemy in offerta a 9,99 Euro potrebbe interesarvi.

Il Black Friday da Udemy è iniziato ufficialmente! Il periodo più ricco di offerte strepitose online include anche la famosa piattaforma di corsi. Tra tutti quelli proposti, in questa occasione specifica proporremo agli appassionati di informatica un brevissimo **corso su Cybersecurity e Privacy** a udemy, per uno sconto del 50%. La sua utilità e completezza, però, lo rendono imperdibile.

Francesco Santin
19 Novembre 2021

NETWORK DIGITAL 360

CYBERSECURITY360

Microsoft Exchange, analisi dell'attacco: ecco perché le patch potrebbero non bastare

Home > Malware e attacchi hacker

L'analisi dell'attacco contro i server Microsoft Exchange condotto mediante lo sfruttamento di alcune vulnerabilità note (e ora risolte), consente di comprendere le tecniche utilizzate dai cyber criminali in modo da adottare le necessarie contromisure. Anche perché le singole patch potrebbero non bastare

02 Apr 2021

P Andrea Pastore
Security Researcher , Exprivia

ASEFI BROKERS
Informazione online dal 2003

Home | Notizie | Insurtech | Interviste | Brokers | Chi siamo | Contatti

Attacchi cyber riusciti in crescita del 56% in Italia, boom violazione privacy

Giovedì, 18 Novembre, 2021 - 08:56 Autore: Gillespie

Sono in costante aumento in Italia gli attacchi cyber che vanno a buon fine, provocando danni a istituzioni, aziende e privati cittadini. È quanto emerge dall'ultimo Rapporto sulle minacce informatiche dell'Osservatorio Cybersecurity di Exprivia, che tra luglio e settembre 2021 ha registrato 273 fenomeni tra attacchi, incidenti e violazioni della privacy.

NETWORK DIGITAL 360

CYBERSECURITY360

Cyber security, tra consapevolezza e sicurezza “by design”: i punti chiave su cui intervenire

Home > Cybersecurity nazionale

La pandemia ha indubbiamente contribuito ad accelerare i processi di digital transformation e migrazione al cloud, ma anche a far crescere il numero di attacchi e incidenti cyber dovuti in buona parte all’incremento di dispositivi connessi in rete. Ecco le soluzioni per una corretta applicazione del paradigma di security by design

11 Mar 2021

Domenico Raguseo
Head of CyberSecurity Exprivia

TRM network

Home Attualità Cronaca Cultura & Spettacolo Politica Scienza e salute Sport Tecnologia & Web

Home » Attualità » Video » Cybersecurity: l’Osservatorio Exprivia presenta i dati del secondo trimestre 2021

Archiviato con: CyberSecurity Exprivia Puglia Sicurezza Informatica

Cybersecurity: l’Osservatorio Exprivia presenta i dati del secondo trimestre 2021

Cybersecurity. L’Osservatorio Exprivia ha presentato i dati del secondo trimestre 2021, certificando

Barisera news

Home In primo piano Attualità Le inchieste Cronaca Bari Calcio Politica Economia School Altro Contatti

A Bari il "Cybersecurity for Digital Trasformation" importante convegno internazionale

Paola Copertino 11/12/2021 Cultura

La globalizzazione ha fatto sì che bisogna pensare allargando confini ed orizzonti. Fondamentale poi fare rete fra enti ed istituzioni per avere uno sguardo di insieme che sia più dettagliato e lungimirante possibile. In questa ottica è stato organizzato un convegno di respiro internazionale.

BitMAT

NEWS INTERNET SICUREZZA CASE HISTORY TECNOLOGIE MERCATO VERTICAL APP

Home › Sicurezza

Incidenti informatici in aumento: +40% le violazioni privacy

Da **Redazione BitMAT** - 15/11/2021

Secondo Exprivia tra luglio e settembre aumentano gli incidenti informatici e i settori più colpiti sono Software/Hardware, Finance e PA.

Sono in costante aumento in Italia gli incidenti informatici, ovvero gli attacchi informatici che vanno a buon fine provocando danni a istituzioni, aziende e privati cittadini. È quanto emerge dall'ultimo **Rapporto sulle minacce informatiche dell'Osservatorio Cybersecurity di Exprivia**, presentato durante **l'Apulia Cybersecurity Forum** nella sede della business school **Spegea** a Bari, che **tra luglio e settembre 2021 registra 273 fenomeni tra attacchi, incidenti e violazioni della privacy**.

TRENDING Remote working ancora poco sicuro

SPECIALE SICUREZZA 360x365

ATTUALITÀ OPINIONI RICERCHE SOLUZIONI

SEI QUI: Home » Speciale Sicurezza » Exprivia avverte: sempre più attacchi vanno a buon fine

SPECIALE SICUREZZA

Exprivia avverte: sempre più attacchi vanno a buon fine

DI REDAZIONE BITMAT — 15 NOVEMBRE 2021 LETTURA 3 MIN

Secondo l'Osservatorio Cybersecurity di Exprivia sono aumentati gli incidenti in rete per i settori Software/Hardware, Finance e PA

Dall'ultimo **Rapporto sulle minacce informatiche dell'Osservatorio Cybersecurity di Exprivia** emerge che in Italia gli incidenti informatici sono in costante aumento provocando danni a istituzioni, aziende e privati cittadini. Tra luglio e settembre 2021, il Rapporto ha, infatti, riporta 273 fenomeni tra attacchi, incidenti e violazioni della privacy.

TRENDING Safer Internet Day: le strategie per la cyber security aziendale ...

LineaEDP DA OLTRE 30 ANNI LA VOCE DEI CIO

CIO CLOUD MERCATO NEWS TECNOLOGIA CASE HISTORY REPORT SICUREZZA IOT

SEI QUI: Home » Rubriche » Sicurezza » Exprivia avverte: sempre più attacchi vanno a buon fine

SICUREZZA

Exprivia avverte: sempre più attacchi vanno a buon fine

DI REDAZIONE LINEAEDP — 15/11/2021 LETTURA 3 MIN

Secondo l'Osservatorio Cybersecurity di Exprivia sono aumentati gli incidenti in rete per i settori Software/Hardware, Finance e PA

Dall'ultimo **Rapporto sulle minacce informatiche dell'Osservatorio Cybersecurity di Exprivia** emerge che in Italia gli incidenti informatici sono in costante aumento provocando danni a istituzioni, aziende e privati cittadini. Tra luglio e settembre 2021, il Rapporto ha, infatti, riporta 273 fenomeni tra attacchi, incidenti e violazioni della privacy.

PassalaParola.net

Cronaca Politica Sport Ambiente Medicina Eno&Gastronomia Cultura Costume In viaggio

CRIMINI INFORMATICI SEMPRE PIÙ SOFISTICATI: AUMENTANO GLI ATTACCHI CHE VANNO A BUON FINE.

Di Redazione Il 15 novembre 2021 In Tecnologia

Sono in costante aumento in Italia gli incidenti informatici, ovvero gli attacchi informatici che vanno a buon fine, provocando danni a istituzioni, aziende e privati cittadini. È quanto emerge dall'ultimo **Rapporto sulle minacce informatiche dell'Osservatorio Cybersecurity di Exprivia**, presentato oggi durante l'Apulia Cybersecurity Forum nella sede **della business school Spegea** a Bari, che tra luglio e settembre 2021 registra 273 fenomeni tra attacchi, incidenti e violazioni della privacy.

Territorio PA

TERRITORIO ARCHITETTURA ECONOMIA ATTUALITÀ AMBIENTE GIORNALE Cosa stai cercando?

Home > Attualità > Attacchi informatici riusciti +56%, boom violazione privacy

Attualità In evidenza

Attacchi informatici riusciti +56%, boom violazione privacy

Novembre 15, 2021 at 8:00 am |

di Antonello Ardito

Sono in costante aumento in Italia gli incidenti informatici, ovvero gli attacchi informatici che vanno a buon fine provocando danni a istituzioni, aziende e privati cittadini. È quanto emerge dall'ultimo Rapporto sulle minacce

il Corriere della Sicurezza
giornale on line
direttore Tiziana Capponi

Home | Primo Piano | Innovazione | Uomini e Mezzi | Attività Internazionale

Home › Aziende › Crimini informatici sempre più sofisticati aumentano gli attacchi che vanno a buon...

Aziende | news | Sicurezza reti | Sistemi e aziende

Crimini informatici sempre più sofisticati aumentano gli attacchi che vanno a buon fine

15 Novembre 2021

redazione

Sono in costante aumento in Italia gli incidenti informatici, ovvero gli attacchi informatici che vanno a buon fine provocando danni a istituzioni, aziende e privati cittadini. È quanto emerge dall'ultimo **Rapporto sulle minacce informatiche dell'Osservatorio Cybersecurity di Exprivia**, presentato oggi durante **l'Apulia Cybersecurity Forum**nella sede della business school Spegea a Bari, che tra luglio e settembre 2021 registra 273 fenomeni tra attacchi, incidenti e violazioni della privacy.

Ansa Industry 4.0 › News

Fai la Ricerca | Vai a ANSA.it

NEWS | STORIE DI IMPRESA | COMPETENZE&TERRITORI | EUROPA 4.0 | I PROTAGONISTI | LE TECNOLOGIE | INTERVISTE | MULTIMEDIA

ANSA.it › Industry 4.0 › News › Cybersecurity: rapporto Exprivia, crescono attacchi efficaci

Cybersecurity: rapporto Exprivia, crescono attacchi efficaci

Tecniche più sosfisticate con danni a istituzioni e privati

Redazione ANSA MILANO 12 NOVEMBRE 2021 14:58

(ANSA) - MILANO, 12 NOV - Sono in costante aumento in Italia gli incidenti informatici, ovvero gli attacchi informatici che vanno a buon fine, provocando danni a istituzioni, aziende e privati cittadini.

È quanto emerge dall'ultimo Rapporto sulle minacce informatiche dell'Osservatorio Cybersecurity di Exprivia, presentato durante l'Apulia Cybersecurity Forum nella sede della business school Spegea a Bari, che tra luglio e settembre 2021 registra 273 fenomeni tra attacchi, incidenti e violazioni della privacy.

la Repubblica

Cybersecurity, Exprivia: "Crescono attacchi efficaci con tecniche più sofisticate e danni a istituzioni e privati"

Secondo il report presentato dall'Osservatorio della società, tra luglio e settembre 2021 sono stati registrati 273 fenomeni fra attacchi, incidenti e violazioni della privacy. E le modalità utilizzate dai cybercriminali sono in costante evoluzione

12 NOVEMBRE 2021 — 1 MINUTI DI LETTURA

Sono in costante aumento in Italia gli incidenti informatici, ovvero gli attacchi informatici che vanno a buon fine, provocando danni a istituzioni, aziende e privati cittadini. È quanto emerge dall'ultimo rapporto sulle minacce informatiche dell'Osservatorio cybersecurity di Exprivia, presentato durante l'Apulia cybersecurity forum nella sede della business school Spegea a Bari. Tra luglio e settembre 2021 sono stati registrati 273 fenomeni fra attacchi, incidenti e violazioni della privacy.

BARI EDIZIONI LOCALI CORRIERE TV ARCHIVIO SERVIZI

CORRIERE DELLA SERA

CORRIERE DEL MEZZOGIORNO / CRONACA

I DATI

Cybersecurity, in Puglia crescono gli incidenti informatici: il rapporto

La ricerca Exprivia dimostra come in tutto il territorio nazionale siano in aumento gli hackeraggi che vanno a buon fine. Trend confermato anche nella regione

Sannioportale.it

NEWS SANITÀ DAL WEB GOSSIP TECNOLOGIA BENESSERE CINEMA TV OROSCOPO + AMATE + VISTE TOOLS

Cybersecurity, attacchi informatici riusciti +56%, boom violazione privacy

Sono in costante aumento in Italia gli incidenti informatici, ovvero gli attacchi informatici che vanno a buon fine provocando danni a istituzioni, aziende e privati cittadini. È quanto emerge dall'ultimo Rapporto sulle minacce informatiche dell'Osservatorio Cybersecurity di Exprivia, che tra luglio e settembre 2021 registra 273 fenomeni tra attacchi, incidenti e violazioni della privacy. Nel complesso i fenomeni sono in lieve diminuzione (-2,5%) rispetto al trimestre precedente, ma le tecniche utilizzate dai cybercriminali, in costante evoluzione, portano a segno ben 93 incidenti.

Puglialive

Home | Archivio | Appuntamenti | Rubriche | Vetrine | Redazioni | Collaboratori | Links | Contatti

Redazione di Bari Cerca nel sito Data Ok

CYBERCRIME: CRESCONO ATTACCHI CHE VANNO A BUON FINE, IN PUGLIA IN MISURA MINORE RISPETTO AL NAZIONALE.

exprivia

12/11/2021

CRIMINI INFORMATICI SEMPRE PIÙ SOFISTICATI:
AUMENTANO GLI ATTACCHI CHE VANNO A BUON FINE

Secondo l'Osservatorio Cybersecurity di Exprivia, presentato oggi a Bari durante l'Apulia Cybersecurity Forum, tra luglio e settembre in Italia aumentano gli incidenti in rete, in particolare per i settori Software/ Hardware, Finance e PA.

Furto dei dati l'illecito più frequente, in crescita le richieste di denaro.
In Puglia il rapporto tra incidenti e attacchi al 40%, più basso rispetto alla media nazionale (56%).

Domenica 06 Febbraio 2022
Aggiornato: 12:26

adnkronos

POLITICA ECONOMIA CRONACA SPETTACOLI SALUTE LAVORO SOSTENIBILITA' INTERNAZIONALE UNIONE EUROPEA PNRR REGIONI

SPORT FINANZA CULTURA IMMEDIAPRESS MOTORI FINTECH MODA MEDIA & COMUNICAZIONE TECH&GAMES MULTIMEDIA

Home Economia

Cybersecurity, attacchi informatici riusciti +56%, boom violazione privacy

12 novembre 2021 | 15.44

Sono in costante aumento in Italia gli incidenti informatici, ovvero gli attacchi informatici che vanno a buon fine provocando danni a istituzioni, aziende e privati cittadini. È quanto emerge dall'ultimo Rapporto sulle minacce informatiche dell'Osservatorio Cybersecurity di Exprivia, che tra luglio e settembre 2021 registra 273 fenomeni tra attacchi, incidenti e violazioni della privacy. Nel complesso i fenomeni sono in lieve diminuzione (-2,5%) rispetto al trimestre precedente, ma le tecniche utilizzate dai cybercriminali, in costante evoluzione, portano a segno ben 93 incidenti.

INFORMAZIONE PER LA SICUREZZA
News web | webtv | magazine

Cerca ...

NEWS » WEBTV » AZIENDE TECNOLOGIE RIVISTA EVENTI CONTATTI

Home » News » Attualità

S NEWS A SICUREZZA 2021: LE NUOVE SFIDE DELLA CYBERSICUREZZA ITALIANA

di Monica Bertolo - 8 Novembre 2021

S News, a **Sicurezza 2021** sul proprio set televisivo allo **Stand M19 – N20** al **Padiglione 5**, approfondirà un tema delicato ed estremamente attuale **MARTEDÌ 23** alle ore **14:00**, nel corso del workshop "**Le nuove sfide della CyberSicurezza italiana**".

MoneyController.it Finanza & Digital Business

Iscritivi alla newsletter Community Chi siamo Dicono di noi Pubblica il tuo profilo

CY4GATE S.p.A.: CY4GATE è sponsor dell' Apulia CyberSecurity Forum 2021

CY4GATE ELETTRONICA GROUP

CY4GATE è sponsor dell' Apulia CyberSecurity Forum 2021

02/11/2021,News

CY4GATE è sponsor dell' Apulia CyberSecurity Forum 2021

Siamo orgogliosi di essere sponsor dell'Apulia CyberSecurity Forum 2021, organizzato dal nostro partner Exprivia dal 9 al 12 novembre.

All'evento è prevista la partecipazione di specialisti del settore che affronteranno temi come: sicurezza, normative, IoT, AI, zero trust e threat Intelligence.

Verrà inoltre presentato il Report dell'Osservatorio Exprivia sulla Cyber Security.

NEWS FORZE ARMATE ~ GEOPOLITICA ~ MONDO MILITARE ~ INDUSTRIA IN EVIDENZA ~

DIFESA ONLINE

CHI SIAMO ANALISI
FOTO E VIDEO APPROFONDIMENTI
EDITORIALE LINKS
LETTERE INTERVISTE

HOME > IN EVIDENZA > EVENTI > ISCRIZIONI ONLINE (GRATUITE) PER "APU...

ISCRIZIONI ONLINE (GRATUITE) PER "APULIA CYBERSECURITY FORUM"

(di Redazione) 25/10/21 - Ottobre è il mese europeo della cybersecurity e sono tante le iniziative pianificate per aumentare la consapevolezza nel settore. *Difesa Online* e SICYNT sostengono ogni iniziativa a favore della diffusione della conoscenza del mondo cyber e delle nuove tecnologie.

MENU | CERCA

la Repubblica

ABBONATI GEDI SMILE

ITALIAN TECH

CERCA

NEWS DATABASE STARTUP VIDEO ITALIENS TUTORIAL PROVE ALMANACCO ITALIAN TECH WEEK CHI SIAMO

LA CURIOSITÀ

Se Mario Draghi va a colazione con gli hacker (buoni)

di Arturo Di Corinto

Il TeamItaly, la Nazionale italiana degli hacker buoni, ha conquistato il terzo posto nelle gare di cybersecurity di Praga. Il presidente del Consiglio li ha ricevuti e si è complimentato con loro

17 OTTOBRE 2021 4 MINUTI DI LETTURA

Pochi lo sanno, ma esiste una nazionale italiana di hacker, è giovane, numerosa e vince pure all'estero. Il primo ottobre, i suoi 10 componenti sono saliti sul podio della maggiore competizione europea, **la European Cyber Security Challenge, come terzi arrivati dopo Germania e Polonia**, anche se fino a poche ore prima si erano meritati il primo posto.

il Corriere della Sicurezza
giornale on line
direttore Tiziana Capponi

Home | Primo Piano | Innovazione | Uomini e Mezzi | Attività Internazionale

Aerospazio: droni a rischio attacco hacker Exprivia ne parla al MAM di Grottaglie

23 Settembre 2021

msn notizie

Così i droni diventano supporto contro le minacce alla sicurezza informatica

Antonio Lo Campo 22/09/2021

Nel corso della cerimonia di apertura delle recenti Olimpiadi di Tokio, 1.824 droni hanno disegnato nel cielo coreografie tanto suggestive quanto impressionanti se si pensa al livello di sofisticazione e tecnologia che abbia potuto supportare un tale spettacolo. Oltre

HOME | CANALI TEMATICI | CULTURA E SPETTACOLI | MAGAZINE | EVENTI | TROVA AUTO | ANNUNCI | VIDEO | LA STAMPA

AGGIORNATO ALLE 11:14 - 07 FEBBRAIO

METEO IL SECOLO XIX ACCEDI

GEDI SMILE | NEWSLETTER | LEGGI IL QUOTIDIANO | ABBONATI | REGALA

GENOVA | PROVINCE | LIGURIA | ITALIA | MONDO | ECONOMIA | SPORT | L'AVVISATORE MARITTIMO | The Medi Telegraph | Cerca

Italia-Mondo » Cronaca

Droni sotto attacco cyber. Più sicurezza informatica

Un meeting internazionale a Grottaglie

Nel corso della cerimonia di apertura delle recenti Olimpiadi di Tokio, 1.824 droni hanno disegnato nel cielo coreografie tanto suggestive quanto impressionanti se si pensa al livello di sofisticazione e tecnologia che abbia potuto supportare un tale spettacolo.

ANTONIO LO CAMPO
22 SETTEMBRE 2021

MENU | CERCA

la Repubblica

ABBONATI | GEDI SMILE | R

Seguici su:

Bari

CERCA

HOME | CRONACA | QUARTIERI | TEMPO LIBERO | SPORT | FOTO | RISTORANTI | VIDEO | ANNUNCI LOCALI | CAMBIA EDIZIONE

Cybersicurezza, droni a rischio hacker. L'appello dal Mam di Grottaglie; "Regolamentare l'uso dei dati raccolti"

▲ (reuters)

Alla fiera dell'aerospazio un panel dedicato alle norme sulla sicurezza dei droni. L'intervento del direttore Cybersecurity di Exprivia, Domenico Raguseo: "Sentiremo parlare di IoD, Internet of Drones"

22 SETTEMBRE 2021

1 MINUTI DI LETTURA

NORBAONLINE

TELENORBA | 2.TELEDUE | TG NORBA 24 | radionorba TV | radionorba

HOME | NEWS | ON DEMAND | LIVE | EDIZIONI LOCALI | SPECIALI

CRONACA | POLITICA | ATTUALITÀ | REGIONE | ECONOMIA | CULTURA | SPETTACOLI | SPORT

Grottaglie, Fiera Aerospazio: la dimostrazione con i droni

22-09-2021

Decolli e atterraggi che si susseguono. Sono droni, piccoli e grandi, con funzionalità diverse, che nel corso della Fiera dell'Aerospazio di Grottaglie dimostrano le capacità funzionali e operative. Ma soprattutto lasciano immaginare il vasto campo di utilizzo nel futuro.

Servizio di Francesco Persiani

Intervista a Domenico Raguseo, Direttore Sicurezza Exprivia

MENU CERCA **LA STAMPA** IL QUOTIDIANO ABBONATI ACCEDI

Droni sotto attacco cyber. Più sicurezza informatica

Un meeting internazionale a Grottaglie

ANTONIO LO CAMPO

22 Settembre 2021 | Modificato il: 22 Settembre 2021 3 minuti di lettura

Nel corso della cerimonia di apertura delle recenti Olimpiadi di Tokio, 1.824 droni hanno disegnato nel cielo coreografie tanto suggestive quanto impressionanti se si pensa al livello di sofisticazione e tecnologia che abbia potuto supportare un tale spettacolo.

24 Italia Attualità

In evidenza In edicola con Il Sole Lab24: i visual Osservatorio PNRR Sanremo 2022

In Puglia

Droni e tecnologie spaziali col Mediterranean Aerospace Matching

Prologo del G20 sull'aerospazio (in programma a ottobre a Roma) e tre giorni di incontri e dimostrazioni a Grottaglie

di Domenico Palmiotti

21 settembre 2021

I punti chiave

- Saccoccia (Asi): ruolo chiave delle attività spaziali
- Verso i network per trasporti spaziali
- Nello spazio con sistemi economici e flessibili
- I droni dell'Enav e quelli israeliani

Nella settimana che vede svolgersi in Italia la seconda edizione del "G20 Space Economy Leaders Meeting" focalizzato sui temi scelti dalla presidenza italiana (People, Planet, Prosperity) e in preparazione del G20 dello spazio in programma a ottobre, la Puglia, con l'iniziativa all'aeroporto

CYBERSECURITYITALIA

Home Italia Europa Mondo Homeland Security Report Eventi Video

TeamItaly, ecco i 10 hacker etici per i campionati europei del 2021

REDAZIONE – 21 SETTEMBRE 2021 – ITALIA

L'Italia ha scelto i 10 hacker etici che parteciperanno all'European cyber security challenge. Le gare si svolgeranno a Praga, in presenza, dal 28 settembre al 1 ottobre e raccoglieranno centinaia di giovani esperti di sicurezza informatica provenienti da oltre venti paesi.

msn notizie

Droni e tecnologie spaziali col Mediterranean Aerospace Matching

di Domenico Palmiotti 21/09/2021

Nella settimana che vede svolgersi in Italia la seconda edizione del "G20 Space Economy Leaders Meeting" focalizzato sui temi scelti dalla presidenza italiana (People, Planet, Prosperity) e in preparazione del G20 dello spazio in programma a ottobre, la Puglia, con l'iniziativa all'aeroporto di Grottaglie del Mediterranean Aerospace Matching (Mam), sarà uno degli snodi importanti.

CYBERSECURITY NATIONAL LABORATORY

CHI SIAMO WEB SERIES ATTIVITÀ FORMAZIONE BANDI E CALL NEWS CONTATTI

Home > Home Gallery > Concluso il ritiro della Nazionale italiana degli hacker etici: ora i campionati europei del 2021

20 Set Concluso il ritiro della Nazionale italiana degli hacker etici: ora i campionati europei del 2021

Anche la nazionale italiana di cybersicurezza, il TeamItaly, parteciperà alla European cyber security challenge, competizione internazionale organizzata dalla European Union Agency for Cybersecurity (Enisa) che decreterà la migliore squadra di hacker etici del Vecchio Continente. Le gare si svolgeranno a Praga, in presenza, dal 28 settembre al 1 ottobre e raccoglieranno centinaia di giovani esperti di sicurezza informatica provenienti da oltre venti paesi.

WIRED SCIENZA ECONOMIA CULTURA GADGET SECURITY DIRITTI IDEE VIDEO PODCAST

REDAZIONE SECURITY 20.09.2021

Scelti i 10 giovani hacker etici del team italiano di cybersecurity

Il Team Italy parteciperà alla European cybersecurity challenge, le gare per decretare la miglior squadra di hacker in Europa, a Praga dal 28 settembre all'1 ottobre

Anche la **nazionale italiana di cybersicurezza, il TeamItaly**, parteciperà alla **European cyber security challenge**, competizione internazionale organizzata dalla European Union Agency for Cybersecurity (Enisa) che decreterà la migliore squadra di hacker etici del Vecchio Continente.

TESTATA DI NETCONSULTING CUBE NEWSLETTER SERVIZI

inno3 innovazione, informazione, incontro

SCENARI TECNOLOGIE GO TO MARKET UTENTI REPORTAGE EDITORIALI CEO CAFÈ CIO CAFÈ ROOM

Home › Tecnologie › Blockchain, ecosistemi e norme certe generano valore

Tecnologie

Blockchain, ecosistemi e norme certe generano valore

E' considerata tecnologia fondamentale per lo sviluppo del Paese, ma progetti ed investimenti sono ancora agli inizi. Gli esperti si confrontano sulla base del whitepaper Anitec-Assinform Attualità e Prospettive della Blockchain per la Crescita dell'Economia italiana

Mario De Ascentiis - 16.09.2021

Tra i **digital enabler** più "discussi" e promettenti, **blockchain** è conosciuta soprattutto per la sua stretta relazione con il mondo delle criptovalute, meno per le tante possibilità di implementazione nei processi di industrie, imprese e PA, che potrebbero beneficiarne in forma esponenziale rispetto a quanto non accade oggi, soprattutto se si pensa al **potenziale di integrazione di blockchain** nei processi di **trasformazione digitale**

LARANEWS DIFESA SICUREZZA CYBER ENERGIA SVILUPPO ORGANIZZATIVO

Cy4Gate firma importanti accordi in ambito Cyber Security e Cyber Intelligence

Set 08 2021 | a cura della Redazione

Fra nuove partnership e commesse per 700.000 euro, gli inizi di settembre hanno portato ulteriori successi alla società controllata da Elettronica, consolidandone il ruolo di primo piano nel mercato internazionale dei prodotti e dei servizi mirati al contrasto della minaccia cibernetica.

il Corriere della Sicurezza

giornale on line

direttore Tiziana Capponi

Home Primo Piano Innovazione Uomini e Mezzi Attività Internazionale

Cy4gate sigla partnership con Exprivia

1 Settembre 2021

redazione

CY4GATE (AIM: CY4) – società attiva nel mercato della cyber intelligence e cyber security a 360° – comunica di aver siglato un accordo di partnership con Exprivia S.p.A. – società italiana quotata in Borsa Italiana nel mercato MTA e a capo di un gruppo internazionale specializzato in Information and Communication Technology.

the GLOBAL eye

Complex and Glocal Thinking, The Science of Where

Friends Menu Cerca

UNCATEGORIZED

Cybersecurity. CY4GATE in partnership con Exprivia per il contrasto alle minacce cyber (Analisi Difesa)

Di Marco Emanuele Settembre 2, 2021 Articolo in evidenza

CY4GATE (AIM: CY4) – società attiva nel mercato della cyber intelligence e cyber security a 360° – comunica di aver siglato un accordo di partnership con Exprivia S.p.A. – società italiana quotata in Borsa Italiana nel mercato MTA e a capo di un gruppo internazionale specializzato in Information and Communication Technology.

Fondato e diretto da Luca Tatarelli

Report Difesa

Geopolitica & Sicurezza

Intelligo ergo scribo

Cerca...

Industrie della Difesa

CY4GATE: ACCORDO DI PARTNERSHIP CON EXPRIVIA PER CONTRASTO A CYBER THREATS

DI REDAZIONE PUBBLICATO IL 1 SETTEMBRE 2021 NESSUN COMMENTO

Roma. CY4GATE, società attiva nel mercato della cyber intelligence e cyber security, ha siglato un accordo di partnership con Exprivia S.p.A., una società italiana quotata alla Borsa Italiana nel mercato MTA e a capo di un gruppo internazionale specializzato in Information and Communication Technology.

NEWS FORZE ARMATE GEOPOLITICA MONDO MILITARE INDUSTRIA IN EVIDENZA

cerca su difesaonline.it

DIFESA ONLINE

CHI SIAMO FOTO E VIDEO EDITORIALE LETTERE

ANALISI APPROFONDIMENTI LINKS INTERVISTE

SOSTIENI DIFESA ONLINE

HOME > IN EVIDENZA > CYBER > IL NUOVO SOC EXPRIVIA: TRA TECNOLOGIA E TE...

IL NUOVO SOC EXPRIVIA: TRA TECNOLOGIA E TERRITORIO

02/09/21 - In questo periodo parlare di Cyber security è sempre più comune, anche se non sempre se ne parla con cognizione di causa.

Questa volta abbiamo pensato di parlarne con Domenico Raguseo, nella sua veste di direttore del nuovo *Security Operation Center* (SOC) di Molfetta.

websim.it

Download Download

Home Free Area Certificates Strategie Turbo FtseMib a leva Websim Journal Notizie Reuters Oggi in Borsa Titoli Caldi

Focus sui mercati Fatti & Effetti Video Research Analisi fondamentale Analisi tecnica ETF Portafogli

Home > Fatti & Effetti

FATTI & EFFETTI

CY4GATE - Accordo di partnership nell'ambito cybersecurity con Exprivia

Redazione 02/09/2021 Ore 09:12

Ottima news

FATTO

Cy4Gate ha annunciato ieri mattina di aver firmato un accordo con Exprivia, società italiana specializzata nell'ICT (ricavi 2020 168 mln). L'accordo prevede in primo luogo la fornitura della soluzione RTA (Real Time Analytics, soluzione di monitoraggio della sicurezza informatica e di tempestiva risposta in caso di incidenti cyber) di Cy4Gate al nuovo SOC (Security Operations Center) di Exprivia, ossia il centro operativo 24/7 che fornisce servizi per la sicurezza informatica di aziende, istituzioni e pubblica amministrazione. Il comunicato stampa non include dettagli sul valore per CY4 del contratto di fornitura della soluzione RTA.

AVIO BLOG *Tutte le ultime notizie Aeronautiche*

Notizie Italia Notizie Estero Media Aeroporti Compagnie Aeree Forze Aeree Incidenti Industria

NOTIZIE ITALIA

Il nuovo SOC Exprivia: tra tecnologia e territorio

BY AVIOBLOG · 2 SEPTEMBER 2021

In questo periodo parlare di Cyber security è sempre più comune, anche se non sempre se ne parla con cognizione di causa.

teleborsa

Cerca notizie, titoli o ISIN

Azioni Milano A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

NOTIZIE QUOTAZIONI RUBRICHE AGENDA VIDEO ANALISI TECNICA STRUMENTI GUIDE PRODOTTI L'AZIENDA

Home Page / Notizie / CY4gate in partnership con Exprivia per sicurezza informatica

CY4gate in partnership con Exprivia per sicurezza informatica

commenta altre news

Finanza - 01 settembre 2021 - 11.50

Argomenti trattati

Exprivia (5)

Titoli e Indici

Cy4gate +0.55% · Exprivia -1.42%

(Teleborsa) - **CY4gate ha siglato un accordo di partnership con Exprivia**. Tra le prime attività che saranno svolte grazie alla nuova partnership vi è l'integrazione della tecnologia proprietaria **RTA** (Real Time Analytics) di Cy4gate **nel nuovo Security Operations Center (SOC)**

Economia | News

CY4gate in partnership con Exprivia per sicurezza informatica

2 Minuti di Lettura

Mercoledì 1 Settembre 2021, 12:00

(Teleborsa) - **CY4gate ha siglato un accordo di partnership con Exprivia.** Tra le prime attività che saranno svolte grazie alla nuova partnership vi è l'integrazione della tecnologia proprietaria **RTA** (Real Time Analytics) di Cy4gate **nel nuovo Security Operations Center (SOC) di Exprivia**, il centro servizi per la sicurezza informatica di aziende, istituzioni e pubblica amministrazione.

CY4gate in partnership con Exprivia per sicurezza informatica

TELEBORSA

Pubblicato il 01/09/2021
Ultima modifica il 01/09/2021 alle ore 11:50

CY4gate ha siglato un accordo di partnership con Exprivia. Tra le prime attività che saranno svolte grazie alla nuova partnership vi è l'integrazione della tecnologia proprietaria **RTA** (Real Time Analytics) di Cy4gate **nel nuovo Security Operations Center (SOC) di Exprivia**, il centro servizi per la sicurezza informatica di aziende, istituzioni e pubblica amministrazione.

CY4GATE in partnership con Exprivia per il contrasto alle minacce cyber

1 settembre 2021 di Redazione in Cyber

CY4GATE (AIM: CY4) – società attiva nel mercato della cyber intelligence e cyber security a 360° – comunica di aver siglato un accordo di partnership con Exprivia S.p.A. – società italiana quotata in Borsa Italiana nel mercato MTA e a capo di un gruppo internazionale specializzato specializzato in Information and Communication Technology.

CY4gate in partnership con Exprivia per sicurezza informatica

(Teleborsa) - CY4gate ha siglato un accordo di partnership con Exprivia. Tra le prime attività che saranno svolte grazie alla nuova partnership vi è l'integrazione della tecnologia proprietaria RTA (Real Time...

Investire sul web

Notizie | Economia e Mercati | Titoli azionari | Criptovalute | Indici azionari | Migliori e Peggiori di Borsa Italiana | Rating | Contatti e Collaborazioni

Privacy Policy

CY4GATE ELETTRONICA GROUP

Cy4Gate azioni – Sigla partnership con Exprivia per il contrasto delle cyber-minacce

Settembre 1, 2021 admin

CYGATE ha firmato un accordo di partnership con Exprivia per il contrasto alle cyber threats. Tra le prime attività prevista dalla nuova collaborazione, vi e' l'integrazione della tecnologie proprietaria RTA (Real Time Analytics) di Cy4Gate nel nuovo Security Operations Center (SOC) di Exprivia. Diciamo in merito che Real Time Analytics (RTA) e' la soluzione sviluppata da CY4GATE per il monitoraggio della sicurezza informatica e per fornire una tempestiva risposta in caso di incidenti cyber. Grazie ad algoritmi di AI e di correlazione, é in grado di acquisire, normalizzare, arricchire, analizzare e indicizzare enormi flussi di cyber eventi in tempo reale, consentendo all'analista di rilevare anomalie e stabilire le condizioni per reagire rapidamente.

AvioNews
World Aeronautical Press Agency

Non riceve alcun finanziamento pubblico
Direttore responsabile:
CLARA MOSCHINI

Home | Notizie | Video | Abbonamenti | Contattaci

Home ▶ Industria ▶ Scienza e tecnologia ▶ Sicurezza

Cy4Gate: siglato accordo partne per contrasto cyber threat

Tra le prime attività svolte integrazione tecnologia proprietaria Rta

Cy4Gate, società attiva nel mercato della cyber intelligence e cybersecurity a 360°, comunica di aver siglato un accordo di partnership con Exprivia SpA, azienda italiana quotata in Borsa Italiana nel mercato Mta ed a capo di un gruppo internazionale specializzato in Information and Communication Technology.

informazione.it Notizie a Confronto

Prima pagina | Ultime notizie | Interno | Esteri | Economia | Scienza... | Spettacolo... | Salute | Sport | Notizie locali

Sicurezza informatica, Exprivia lancia il Soc: un centro servizi per proteggere aziende ed enti pubblici

29/07/2021 - 03:50 ECONOMIA

È uno dei motivi che ha portato Exprivia a lanciare nella sua sede di Molfetta il nuovo Security operations center (SOC) un centro servizi per la tutela della sicurezza di aziende, istituzioni e pubblica amministrazione.

BitMAT | BitMATv | Top Trade | Linea EDP | Itis Magazine | Speciale Sicurezza | Industry 4.0 | Sanità Digitale | Redazione | Contattaci

TRENDING Safer Internet Day: le strategie per la cyber security aziendale nell'era ...

EDP DA OLTRE 30 ANNI LA VOCE DEI CIO

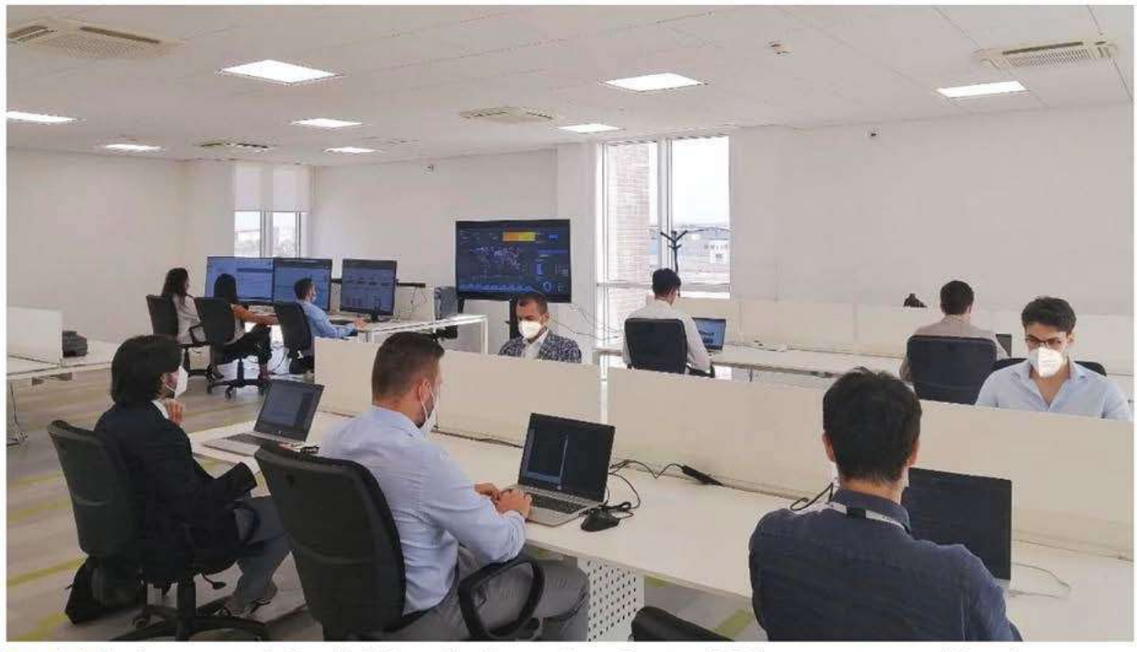
CIO | CLOUD | MERCATO | NEWS | TECNOLOGIA | CASE HISTORY | REPORT | SICUREZZA | IOT

UNCATEGORIZED

Exprivia inaugura un SOC in Puglia

DI REDAZIONE LINEAEDP – 23/07/2021 LETTURA 4 MIN

Inaugurato a Molfetta, già sede del quartier generale dell'azienda, il Security Operations Center (SOC) di Exprivia



Exprivia ha inaugurato in Puglia il **Security Operations Center (SOC)**, un centro servizi per la sicurezza informatica di aziende, istituzioni e pubblica amministrazione.

07 Febbraio 2022 | 10:49

BANCAFORTE innovation key

Temi Speciali eventi Rubriche Bancaforte TV Iscriviti alla Newsletter

Trend topics Covid-19 Credito PSD2 Fintech Blockchain

SICUREZZA

Cybersecurity, apre in Puglia il Soc di Exprivia

di Flavio Padovan - 27 Luglio 2021

Al servizio di aziende, banche, istituzioni e PA, opererà per prevenire e difendere dalle minacce cyber, identificare le compromissioni dei sistemi informatici, rispondere agli attacchi e ripristinare i servizi. Secondo i dati dell'Osservatorio Cybersecurity di Exprivia, nel secondo trimestre 2021 gli incidenti sono aumentati del 300%

Opererà dalla Puglia il Security Operations Center (SOC) di Exprivia. Sarà infatti Molfetta a ospitare il centro servizi per la sicurezza informatica di aziende, banche, istituzioni e pubblica amministrazione. Un laboratorio dove un team di esperti svolgerà attività di monitoraggio e analisi delle vulnerabilità h24, 7 giorni su 7, per prevenire e difendere dalle minacce. Inoltre, grazie a sofisticate tecnologie di intelligence, si potranno identificare le compromissioni dei sistemi informatici per rispondere agli attacchi e ripristinare i servizi, ampliando l'offerta di servizi già erogati da remoto a clienti italiani e internazionali.

MENU | CERCA

la Repubblica

ABBONATI GEDI SMILE | R | ACCEDI

Seguici su:

Bari

CERCA

HOME CRONACA QUARTIERI TEMPO LIBERO SPORT FOTO RISTORANTI VIDEO ANNUNCI LOCALI CAMBIA EDIZIONE

27 LUGLIO 2021

Sicurezza informatica, Exprivia lancia il Soc: un centro servizi per proteggere aziende ed enti pubblici

▲ Gli analisti del Soc al lavoro nella sede di Exprivia a Molfetta

di Gianvito Rutigliano

Con la crescita dello smart working, della Dad e dell'utilizzo dei servizi digitali le vulnerabilità si sono moltiplicate. Il nuovo Security operation center nato a Molfetta monitora i sistemi informatici dei clienti. "Attacchi hacker in aumento"

PassalaParola.net

Cronaca | Politica | Sport | Ambiente | Medicina | Eno&Gastronomia | Cultura | Costume | In viaggio | in Esclusiva | Chi siamo

CYBERSECURITY: EXPRIVIA APRE IN PUGLIA IL SECURITY OPERATIONS CENTER

Di Redazione Il 23 luglio 2021 In Sicurezza E Lavoro

Apre in Puglia il **Security Operations Center (SOC) di Exprivia**, il centro servizi per la sicurezza informatica di aziende, istituzioni e pubblica amministrazione. Cresce l'attenzione per la difesa dai crimini in rete, in costante aumento nell'ultimo anno, e il team di esperti in sicurezza di Exprivia mette a disposizione le proprie competenze attraverso un laboratorio che lavorerà h24, 7 giorni su 7, ampliando l'offerta di servizi già erogati da remoto a clienti italiani e internazionali.

il Corriere della Sicurezza
giornale on line
direttore Tiziana Capponi

Home | Primo Piano | Innovazione | Uomini e Mezzi | Attività Internazionale

Aziende | Sicurezza reti | Sistemi e aziende

Picco di incidenti informatici tra aprile e giugno, Exprivia apre centro servizi per la sicurezza di aziende, istituzioni e pa

23 Luglio 2021

redazione

Apre in Puglia il **Security Operations Center (SOC) di Exprivia**, il centro servizi per la sicurezza informatica di aziende, istituzioni e pubblica amministrazione. Cresce l'attenzione per la difesa dai crimini in rete, in costante aumento nell'ultimo anno, e il team di esperti in sicurezza di Exprivia mette a disposizione le proprie competenze attraverso un laboratorio che lavorerà h24, 7 giorni su 7, ampliando l'offerta di servizi già erogati da remoto a clienti italiani e internazionali.

MF MILANO FINANZA CLASS CNBC

OPTIONS OF next35

Accedi | Registrati | Abbonati

News Business Mercati Ricerca titoli Il Trader In Gestione Growth Italia Osservatori Edicola Strumenti My Tech Opinioni Lifestyle Class CNBC Live

MF ONLINE

Secondo l'Osservatorio Exprivia, il banking online e le attività di delivery sono risultati i settori più colpiti in Italia

Cybercrime, gli attacchi riusciti crescono del 300%

di Nicola Carosielli

MF - Numero 143 pag. 9 del 22/07/2021

/ MF Online / Cybercrime, gli attacchi riusciti crescono del 300%

L'iperconnessione dettata, nell'ultimo anno, dall'aumento del tempo passato online e dalla massiccia diffusione di smart working e servizi digitali, fa crescere il rischio di esposizione cyber e il conseguente interesse sul tema della difesa di dispositivi e sistemi. Stando a quanto rilevato dall'ultimo Rapporto sulle minacce informatiche dell'Osservatorio Cybersecurity di Exprivia,...;

NEWS CORRELATE vedi tutte

Fineco, il consenso stima ricavi nel quarto trimestre in aumento a 200 milioni

DIRETTORE: FILIPPO ASTONE

LUNEDÌ 7 FEBBRAIO 2022, 11:52

INDUSTRIA ITALIANA

ANALISI E NEWS SU ECONOMIA REALE, AUTOMAZIONE, INNOVAZIONE, B2B TECH

HOME INDUSTRIA DIGITAL TRANSFORMATION & ICT AUTOMAZIONE, ROBOT & I.A. ECONOMIA ITALIANA

DIGITAL TRANSFORMATION & ICT

Nasce in Puglia il Security Operations Center di Exprivia

All'interno del Soc un team di esperti sarà a disposizione dei clienti italiani e internazionali

22 Luglio 2021

Il Soc di Exprivia a Molfetta

Exprivia ha inaugurato in Puglia un Security Operations Center (Soc) di Exprivia, un centro servizi per la sicurezza informatica di aziende, istituzioni e pubblica amministrazione. Il team di esperti in sicurezza di Exprivia mette così a disposizione le proprie competenze attraverso un laboratorio che lavorerà h24, 7 giorni su 7, ampliando l'offerta di servizi già erogati da remoto a clienti italiani e internazionali. Il Soc svolgerà attività di monitoraggio e analisi delle vulnerabilità per prevenire e difendere dalle minacce; inoltre, dotato di sofisticate tecnologie di intelligence, il team di esperti potrà identificare le compromissioni dei sistemi informatici per rispondere agli attacchi e ripristinarei servizi.

lunedì, 07 febbraio 2022

Seguici su

IL GIORNALE D'ITALIA

Il Quotidiano Indipendente

Cerca...

"La libertà al singolare esiste solo nelle libertà al plurale" Benedetto Croce

Politica Esteri Cronaca Economia Sostenibilità Innovazione Lavoro Salute Cultura Costume Spettacolo Sport Motori iGdI TV

Exprivia apre il Security Operations Center in Puglia per la sicurezza di aziende, istituzioni e pa

Raguseo: "Il gruppo di esperti coinvolti nel SOC, è costituito da professionisti nel settore della cybersecurity. Lavoriamo con un portfolio di oltre 50 clienti in Italia e all'estero "

22 Luglio 2021

ASSINEWS.it
il quotidiano assicurativo

Cybercrime, gli attacchi riusciti crescono del 300%

22 Luglio 2021

SECONDO L'OSSERVATORIO EXPRIVIA, IL BANKING ONLINE E LE ATTIVITÀ DI DELIVERY SONO RISULTATI I SETTORI PIÙ COLPITI IN ITALIA

di Nicola Carosielli

L'iperconnessione dettata, nell'ultimo anno, dall'aumento del tempo passato online e dalla massiccia diffusione di smart working e servizi digitali, fa crescere il rischio di esposizione cyber e il conseguente interesse sul tema della difesa di dispositivi e sistemi. Stando a quanto rilevato dall'ultimo Rapporto sulle minacce informatiche dell'Osservatorio Cybersecurity di Exprivia, nonostante il trend altalenante negli ultimi sei mesi dell'anno, tra aprile e giugno 2021 si sono registrati 280 fenomeni tra attacchi, incidenti e violazioni della privacy con un picco di incidenti (attacchi andati a buon fine) cresciuto di oltre il 300% rispetto al trimestre precedente (da 22 a 90), rivelandosi il dato peggiore degli ultimi 12 mesi. Come spiegato da Domenico Raguseo,

ILIKEPUGLIA
Dir.: A.FERRETTI Facciamo Notizie

Exprivia apre in Puglia il Security operations center per la sicurezza di aziende, istituzioni e PA

Avrà base a Molfetta, già sede del quartier generale dell'azienda, dove un team di esperti sarà a disposizione dei clienti italiani e internazionali

Pubblicato il **22/07/2021** di **Redazione**

NETWORK DIGITAL 360

INTERNET 4.THINGS

Direttore Responsabile: Maria Teresa Della Mura

INDUSTRY 4.0 SMART CITY MOBILE WEARABLE SMART BUILDING SMART AGRIFOOD SMART HEALTH ...

TOPICS Smart Home RFID Industria 4.0 5G Digital transformation Li-Fi Cloud White Paper e Libri Blockchain PA 4.0 Big D

.sicurezza iot

SECURITY

IoT security, cos'è la sicurezza nell'Internet of Things e come proteggersi dagli attacchi

Più aumenta il numero di dispositivi online capaci di interagire attraverso la connettività IoT, più crescono rischi e cyber minacce contro device e app IoT. La diffusione dei dispositivi IoT pone alla ribalta numerose nuove problematiche in termini di sicurezza, privacy e conformità per le aziende di tutto il mondo

di Mirella Castigli, giornalista 9 Luglio 2021

SportsGaming.win XBOX PLAYSTATION ESPORTS WINDOWS ABOUT CONTACT

GAMING

Who are the young ethical hackers who won the national cybersecurity competition

The team of the University of Cagliari imposes itself at Cyberchallenge, the training school to introduce young people to IT security

Team Cagliari (Cyberchallenge) The fifth edition of CyberChallenge.IT ended with a participatory online ceremony , the Italian training school for young ethical hackers of the future.

Parte del gruppo GEDI e la Repubblica

LA PREMIAZIONE

CyberChallenge.IT, ecco il podio degli hacker etici italiani

Gli hacker etici dell'Università di Cagliari

In presenza di autorità e accademici, il vicedirettore generale del Dis, Roberto Baldoni, ha premiato i campioni di CyberChallenge.IT, la scuola della cybersicurezza italiana

09 LUGLIO 2021 — 2 MINUTI DI LETTURA

L'Università di Genova, il Politecnico di Torino e, al primo posto, l'Università di Cagliari: è questo il podio della quinta edizione di CyberChallenge.IT, la scuola di formazione italiana per i giovani hacker etici del futuro.

REDAZIONE SECURITY 08.07.2021

Chi sono i giovani hacker etici che hanno vinto la gara nazionale di cybersecurity

Il team dell'Università di Cagliari si impone a Cyberchallenge, la scuola di formazione per introdurre i giovani alla sicurezza informatica

Team Cagliari (Cyberchallenge)

Si è conclusa con una partecipata cerimonia online la quinta edizione di **CyberChallenge.IT**, la scuola di formazione italiana per i giovani hacker etici del futuro. In presenza di autorità e rappresentanti del mondo accademico e industriale, il Vice direttore generale del Dipartimento delle informazioni per la sicurezza (Dis), ha annunciato le tre squadre del medagliere nazionale: l'Università di Genova, il Politecnico di Torino e l'Università di Cagliari, che hanno conquistato rispettivamente il terzo, il secondo e il primo posto.

RELAZIONE ANNUALE 2020

Garante Privacy, il discorso del Presidente Pasquale Stanzione

di **Redazione Key4biz** | 2 Luglio 2021, ore 14:00

Il discorso integrale del Presidente del Garante Privacy Pasquale Stanzione in occasione della Relazione Annuale 2020 alla Camera.

Signor Presidente della Camera, Autorità, Signore e Signori, la presentazione di questa relazione ha un significato particolare, perché nel delineare l'orizzonte del nostro mandato esprime la consapevolezza dei temi, delle urgenze, dei problemi che questo primo anno di lavoro molto intenso ci ha offerto.

L'autore

Redazione Key4biz

ICT Security MAGAZINE

Home | Articoli | Rubriche | Notizie | Eventi | Newsletter

Cybersecurity per la Blockchain e la Blockchain per la cybersecurity (1/3)

A cura di: Rosita Galiandro - Pubblicato il 25 Maggio 2021

Introduzione

Di solito quando una nuova architettura e tecnologia vengono inserite nel mercato, le persone pensano ai vantaggi e all'innovazione trascurando un aspetto molto importante: la sicurezza informatica della nuova soluzione. Questo non è però un aspetto peculiare dell'informatica, ahimè è valido in generale in molti contesti.

ICT Security MAGAZINE

Home | Articoli | Rubriche | Notizie | Eventi | Newsletter

Cybersecurity per la Blockchain e la Blockchain per la cybersecurity (2/3)

A cura di: Rosita Galiandro - Pubblicato il 14 Giugno 2021

Introduzione

La Blockchain è particolarmente attraente per gli attaccanti perché le transazioni fraudolente non possono essere annullate come spesso possono essere nel sistema finanziario tradizionale. Oltre a ciò, sappiamo da tempo che proprio come la Blockchain ha caratteristiche di sicurezza uniche, ha anche vulnerabilità uniche.

ICT Security MAGAZINE

Home | Articoli | Rubriche | Notizie | Eventi | Newsletter

Cybersecurity per la Blockchain e la Blockchain per la cybersecurity (3/3)

A cura di: Rosita Galiandro - Pubblicato il 5 Luglio 2021

Introduzione

La blockchain **rappresenta un approccio innovativo alla cyber security** perché è una tecnologia che permette di progettare sistemi rispettando il principio security by design.

La sicurezza della tecnologia Blockchain si basa principalmente su tre elementi fondamentali:

CYBERSECURITY NATIONAL LABORATORY

CHI SIAMO | WEB SERIES | ATTIVITÀ | FORMAZIONE | BANDI E CALL | NEWS | CONTATTI

29 Giu CyberChallenge.IT: la scuola degli hacker etici verso la gara finale

Il prossimo **7 luglio** si terrà, in remoto, la **finale di CyberChallenge.IT**: percorso di formazione gratuito per i giovani hacker etici italiani.

WOMEN for Security

Home | CyberLadies | Tavoli di Lavoro | Press e News | Contatti

Extortionware – dal Dark Web "la strategia della vergogna"

Pubblicato da **Annamaria Gigante** | 15/06/2021

I crimini informatici sono fenomeni in continua crescita; ciò in ragione del fatto che il rischio associato alla commissione del reato è basso rispetto ai guadagni che ne derivano. Infatti il cyber crime è oggi un business globale da 600 miliardi di dollari che rappresenta lo 0,8% del PIL mondiale.

NETWORK DIGITAL 360

RM RISK MANAGEMENT 360

Enterprise Risk Management | Compliance | Risk Technology | Risk Assessment | Ricerche e Report

Data breach, le sanzioni comminate dal Garante della Privacy

Home > Analisti Ed Esperti

A partire da gennaio 2021 in Italia sono state comminate precisamente 29 sanzioni da parte del Garante della Privacy, 7 nel primo mese dell'anno, 12 a febbraio, 7 a marzo, 3 ad aprile, per un totale di 7.893.280 euro. Al primo posto la PA, seguita dal settore sanitario.

11 Giu 2021

Fabiano Vincenzo Malerba
Cybersecurity Researcher Expriv

Approfondimenti

D data breach | D data privacy | D data protection | S sanità

Articoli correlati

Privacy
Il riconoscimento facciale negli stadi di calcio, tra privacy e sicurezza
02 Apr 2021

Normative
Sanzioni e attività ispettive in materia di sanità pubblica e impatto sulla protezione dei dati personali
17 Set 2020

Cybersicurezza – Tra Sparta e Atene il fronte aperto delle aziende: l'opinione di Domenico Raguseo di Exprivia

29 maggio 2021 Guiomar Parada

App, Best practices, Big data, Consumatori, Cyber crimine, Digitalizzazione, Fabbriche, Governo, IIoT, Imprese, Industria, Industria 4.0, Infrastrutture, Innovazione, Internet, Investimenti, IoT, Manifattura, Piattaforme, Privato, Pubblico, Regolamentazione, Reti, Salute, Security, Senza categoria, Sicurezza, Virus

"La più grande campagna di **spionaggio** dei tempi recenti ", ha detto dell'attacco **SolarWinds** Thomas Rid, professore di Studi strategici alla **Johns Hopkins.**

BANCAFORTE innovation key

Temi Speciali eventi Rubriche Bancaforte

Trend topics Covid-19 Credito PSD2 Fintech Blockchain

BANCAFORTE TV

Cybersecurity: crescono gli attacchi, ma gli incidenti rimangono costanti

di Flavio Padovan Maddalena Libertini *21 Maggio 2021*

La cyber criminalità ha già voltato pagina rispetto al Covid: ormai gli attacchi che utilizzano temi legati alla pandemia per ingannare gli utenti sono solo un piccola parte. Mentre è ridiventato preponderante – con una crescita molto significativa – il fishing a sfondo finanziario. A rivelarlo è **Domenico Raguseo, Head of Cybersecurity Unit Exprivia**, che anticipa a Bancaforte alcune delle evidenze dell'Osservatorio sulla Cybersecurity che sarà presentato a **Banche e Sicurezza 2021**.

INTERNET 4.THINGS

Direttore Responsabile: **Maria Teresa Della Mura**

INDUSTRY 4.0 SMART CITY MOBILE WEARABLE SMART BUILDING SMART AGRIFOOD SMART HEALTH

.sicurezza iot

SECURITY

La sicurezza dei dispositivi IoT, un fattore sottovalutato

La governance e la conoscenza delle architetture e degli standard utilizzati nell'industria devono suggerire una fortissima specializzazione dei controlli di sicurezza generale. È necessario identificare i responsabili della sicurezza dei dispositivi IoT ma anche creare una cultura della sicurezza informatica

di Domenico Raguseo, Exprivia 18 Maggio 2021

ItaliaOggi

QUOTIDIANO ECONOMICO, GIURIDICO E POLITICO

Home News Banche Dati Politica Marketing Fisco Lavoro EntiLocali Scuola Agricoltura Appalti Guide Edicola My IO

Politica Attualità estero Marketing Economia Diritto e Fisco Diritto e Sport Fisco Giustizia PA Lavoro Professioni Ordini e Associazioni Scuola Agricoltura Contabilità Europa

ITALIAOGGI SETTE - NUMERO 114 PAG. 7 DEL 17/05/2021

Il trend registrato nel report Exprivia: 349 eventi in tre mesi (+612% rispetto al 2020)

Crimini informatici senza freni

Ma inizia la flessione degli attacchi andati a buon fine

Pagina a cura di Antonio Longo

ASSINEWS.it
il quotidiano assicurativo

HOME NEWS RIVISTA TECNICA E NORME MERCATO NEWSLETTER ANNUNCI ESPERTORISPONDE ABBONATI!

Home › Tecnica assicurativa › Assicurazione Danni › Crimini informatici senza freni

Crimini informatici senza freni

17 Maggio 2021

Il trend registrato nel report Exprivia: 349 eventi in tre mesi (+612% rispetto al 2020)
Ma inizia la flessione degli attacchi andati a buon fine
Pagina a cura di Antonio Longo

Da gennaio a marzo in Italia si sono registrati 349 eventi tra cyber-attacchi, incidenti e violazioni della privacy, con una crescita del 47% sul trimestre precedente e ben sette volte di più rispetto ai primi tre mesi del 2020.

FEDERPRIVACY

Area Riservata | Eventi in Agenda | Registro Soci | Shop Online

Home Associazione Attività Informazione Strumenti Community Domande Frequenti

NEWS Cookie: Google rassicura che intende adeguarsi al Gdpr ma gli editori si oppongono

Cyber attacchi nel I° trimestre 2020 +612% rispetto allo scorso anno, ma in flessione quelli riusciti

Privacy & Società Lunedì, 17 Maggio 2021 07:30

Da gennaio a marzo in Italia si sono registrati 349 eventi tra cyber-attacchi, incidenti e violazioni della privacy, con una crescita del 47% sul trimestre precedente e ben sette volte di più rispetto ai primi tre mesi del 2020.

ASSINEWS.it
il quotidiano assicurativo

HOME NEWS RIVISTA TECNICA E NORME MERCATO NEWSLETTER ANNUNCI ESPERTORISPONDE ABBONATI!

Home › Tecnica assicurativa › Assicurazione Danni › Cybercrime, gli attacchi riusciti crescono del 300%

Rapporto Exprivia: in calo le offensive "a tema Covid", ma crescono del 47% i cyber attacchi in tre mesi

13 Maggio 2021

Nel **primo trimestre del 2021** i **cyber attacchi** hanno registrato una crescita del **47%** rispetto e si sono moltiplicati per sette rispetto al periodo gennaio-marzo del al trimestre precedente, 2020.

Conquiste del Lavoro

Quotidiano di informazione socio-economica

Sindacato Economia Vertenze Global Cultura Politica Dibattito Contratti Attualità Pubblico Impiego Pensioni

Cybersecurity

Con la pandemia in aumento i furti dei dati personali

Più smartphone, più smart working e più consumi digitali. La pandemia ha accelerato le trasformazioni delle abitudini e stili d i vita privilegiando acquisti, consumi ed esperienze da web e device. Sta di fatto che, nei primi mesi del 2021, si registra un balzo in avanti degli attacchi informatici in Italia. Lo conferma un report dell'Osservatorio Cybersecurity di Exprivia che prende in esame anche 86 fonti pubbliche. Ebbene, nel periodo gennaio-marzo 2021

Sbircia la notizia Magazine

CORONAVIRUS ULTIMA ORA CRONACA POLITICA REGIONI SALUTE ESTERI SPETTACOLO

Exprivia, nuovo balzo cyber attacchi in Italia

Pubblicato il 11 Maggio 2021, 18:21

Sono stati 349 da gennaio a marzo 2021, sette volte di più rispetto ai primi tre mesi del 2020. Nel mirino App, social e banking online.

Continua a crescere il trend degli attacchi informatici in Italia anche nel 2021. Da quanto emerge nel primo rapporto del 2021 sulle minacce informatiche in Italia elaborato dall'Osservatorio Cybersecurity di Exprivia, nel periodo gennaio-marzo 2021 si sono registrati 349 eventi, tra attacchi, incidenti e violazioni della privacy. Si tratta di una crescita del 47% sul trimestre precedente e sette volte di più rispetto ai primi tre mesi del 2020.

BitMAT

NEWS INTERNET SICUREZZA CASE HISTORY TECNOLOGIE MERCATO VERTICAL APP

Attacchi informatici in crescita del 47% in Italia

Da **Redazione BitMAT** - 07/05/2021

Messaggistica istantanea, social network e banking online le vittime preferite

Attacchi informatici in crescita anche nel 2021 nel nostro paese. Da quanto emerge nel primo rapporto del 2021 sulle minacce informatiche in Italia elaborato dall'Osservatorio Cybersecurity di Exprivia, nel periodo gennaio-marzo 2021 si sono registrati 349 eventi, tra

NETWORK DIGITAL 360

CORCOM

Digital Economy Telco Industria 4.0 PA Digitale Space economy Green economy Finance Videointerviste

IL REPORT

Cybersecurity, attacchi e incidenti moltiplicati per sette nell'ultimo anno

Home > Cyber Security

Il rapporto Exprivia sul primo trimestre 2021: in calo le offensive "a tema Covid". Ma complessivamente si registra un +47% in tre mesi. Domenico Raguseo: "Preoccupante mancanza di consapevolezza sui rischi da parte delle vittime"

07 Mag 2021

IL GIORNALE DELLE PMI

CRESCIMPRESA INFOIMPRESA INNOVAZIONE EXPORT IN DIGITALE INTERNAZIONALIZZAZIONE INTERVISTE TECNOLOGIA

Nuovo balzo di attacchi informatici in Italia nei primi mesi dell'anno: il cybercrime colpisce app, social e banking online

Redazione 7 Maggio 2021

Continua a crescere il trend degli attacchi **informatici in Italia** anche nel 2021. Da quanto emerge nel primo rapporto del 2021 sulle minacce informatiche in Italia elaborato dall'**Osservatorio Cybersecurity di Exprivia**, nel periodo **gennaio-marzo 2021** si sono registrati **349 eventi**, tra attacchi, incidenti e violazioni della privacy. Si tratta di una crescita del 47% sul trimestre precedente e sette volte di più rispetto ai primi tre mesi del 2020. A un anno dallo scoppio della pandemia che ha portato alla massiccia diffusione dello smart working e al ricorso sempre più frequente a servizi online, il cybercrime continua a colpire spesso utilizzando

securityopenlab

Home | Tecnologie/Scenari | Vulnerabilità | Consumer | Sicurezza fisica | Normative | Busine

Cyber attacchi in Italia nel 2021: colpiti app, social e banking

Redazione SecurityOpenLab 07-05-2021

I cyber attacchi continuano a crescere nel primo trimestre 2021: il furto dei dati è in cima alla classifica dei danni.

Nel primo trimestre 2021 sono calati gli attacchi a tema COVID, ma sono aumentati quelli indirizzati al furto di dati. Complessivamente nel periodo indicato la crescita dei cyber attacchi è stata pari al 47% rispetto al trimestre precedente e sette volte più alta rispetto ai primi tre mesi del 2020.

Le informazioni sono contenute nel *Threat Intelligence Report* elaborato dall'Osservatorio Cybersecurity di Exprivia, che ha conteggiato 349 eventi fra gennaio e marzo 2021 tra attacchi, incidenti e violazioni della privacy. Nonostante le percentuali indicate sopra, **il numero medio di attacchi andati a buon fine registra una flessione del 18%** rispetto al trimestre precedente, pur restando in media rispetto all'intero 2020.

NETWORK G11 MEDIA: | CHANNELCITY | IMPRESACITY | GREENCITY | CHANNELCITY MAGAZINE | IMPRESACITY MAGAZINE | SECURITYOPENLAB

BiT city Newsletter Cerca

PRODOTTI | MOBILE | DIGITAL LIFE | GAMING

Homepage > Notizia

Exprivia: nuovo balzo di attacchi informatici in italia

L'Osservatorio Cybersecurity di Exprivia registra nel primo trimestre dell'anno 349 eventi criminali, in continua crescita rispetto al 2020. Calano i crimini informatici a tema Covid. Il furto dei dati è in cima alla classifica dei danni.

Autore: Redazione BitCity

Pubblicato il: 07/05/2021

Digital Life

Continua a crescere il trend degli attacchi **informatici in Italia** anche nel 2021. Da quanto emerge nel **primo rapporto del 2021 sulle minacce informatiche in Italia** elaborato dall'**Osservatorio Cybersecurity di Exprivia**, nel periodo **gennaio-marzo 2021** si sono registrati **349 eventi**, tra attacchi, incidenti e violazioni della privacy. Si tratta di una crescita del 47% sul trimestre precedente e sette volte di più rispetto ai primi tre mesi del 2020.

MENU | CERCA

la Repubblica

Seguici su:

Bari

CERCA

HOME CRONACA QUARTIERI TEMPO LIBERO SPORT FOTO RISTORANTI VIDEO ANNUNCI LOCALI CAMBIA EDIZIONE

Il Covid fa schizzare i crimini informatici in Italia: +47% fra gennaio e marzo 2021

Lo certifica il rapporto dell'Osservatorio cybersecurity di Exprivia. Furto dei dati personali e di denaro sono fra i cyber reati più diffusi anche a causa di smart working e didattica a distanza

06 MAGGIO 2021 — 1 MINUTI DI LETTURA

Nel primo trimestre 2021 in Italia ci sono stati 349 crimini informatici tra attacchi, incidenti e violazioni della privacy, con un balzo in avanti del 47 per cento rispetto al 2020.

DMO Data Manager Online
il portale dell'ICT professionale

SOFTWARE HARDWARE WEB E SOCIAL MERCATO IT TOP100 WHITE PAPERS #WECHANGEIT

Home › Software › Sicurezza › Nuovo balzo di attacchi informatici in Italia nei primi mesi dell'anno

Software Sicurezza

Nuovo balzo di attacchi informatici in Italia nei primi mesi dell'anno

Di **Redazione Data Manager Online** - 6 Maggio 2021

L'Osservatorio Cybersecurity di Exprivia registra nel primo trimestre dell'anno 349 eventi criminali, in continua crescita rispetto al 2020. Calano i crimini informatici a tema Covid. Il furto dei dati è in cima alla classifica dei danni

ASSINEWS.it
il quotidiano assicurativo

HOME NEWS RIVISTA TECNICA E NORME MERCATO NEWSLETTER ANNUNCI ESPERTORISPONDE ABBONATI!

Attacchi informatici, +47% nel trimestre

7 Maggio 2021

di Nicola Carosielli

App, social e banking online sono stati le prime vittime degli attacchi informatici in Italia nel primo trimestre. Secondo l'Osservatorio Cybersecurity di Exprivia, tra gennaio e marzo si sono registrati 349 eventi tra attacchi, incidenti e violazioni delle privacy, in crescita del 47% sul trimestre precedente e di sette volte rispetto a un anno prima.

MF MILANO FINANZA Class CNBC

OPTIONS OF next35

Accedi Registrati Abbonati

News Business Mercati Ricerca titoli Il Trader In Gestione Growth Italia Osservatori Edicola Strumenti My Tech Opinioni Lifestyle Class CNBC Live

MF ONLINE

Attacchi informatici, +47% nel trimestre

di Nicola Carosielli

MF - Numero 089 pag. 17 del 07/05/2021

/ MF Online / Attacchi informatici, +47% nel trimestre

App, social e banking online sono stati le prime vittime degli attacchi informatici in Italia nel primo trimestre. Secondo l'Osservatorio Cybersecurity di Exprivia, tra gennaio e marzo si sono registrati 349 eventi tra

NEWS CORRELATE vedi tutte

Morgan Stanley: il settore Ue dei video games è ipervenduto

Ubs, petrolio a 80 dollari al barile nei prossimi due anni. Eni tra i titoli migliori del settore

Focus sul settore auto

Fineco, il consenso stima ricavi nel

HOME MAIL NOTIZIE FINANZA SPORT CELEBRITY STYLE ALTRO...

yahoo!notizie

Home Notizie Coronavirus Vaccini Vuoi essere Green? Finanza Sport Meteo Grande Fratello Vip 6 Seguici su Instagram Italia ...

Adnkronos

Exprivia, nuovo balzo cyber attacchi in Italia

webinfo@adnkronos.com (Web Info)

6 maggio 2021 · 4 minuto per la lettura

Continua a crescere il trend degli attacchi informatici in Italia anche nel 2021. Da quanto emerge nel primo rapporto del 2021 sulle minacce informatiche in Italia elaborato dall'Osservatorio Cybersecurity di Exprivia, nel periodo gennaio-marzo 2021 si sono registrati 349 eventi, tra attacchi, incidenti e violazioni della privacy. Si tratta di una

GIOVINAZZOLIVE.it

News Sport Mondo Imprese Eventi Città Rubriche Annunci Media Utilità

Cronaca Politica Attualità Cultura Spettacolo Redazionali Longform Storie D'Imprese

Il report

Covid-19: +47% crimini informatici fra gennaio e marzo 2021

Furto dei dati personali e di denaro sono fra i cyber reati più diffusi

CRONACA Giovinazzo venerdì 07 maggio 2021 di La Redazione

Secondo l'ultimo report dell'Osservatorio cybersecurity di Exprivia nel primo trimestre 2021 in Italia ci sono stati 349 crimini informatici tra attacchi, incidenti e violazioni della privacy, con un balzo in avanti del 47 per cento rispetto al 2020.

raquadra.info

SOCIAL MEDIA

il giornale on-line fondato dalla giornalista Lilli D'Amicis

SEZIONI APERTAMENTE & PARLA CON ME VIDEO SPECIALI ORAQUADRA CONTATTI & SEGNALAZIONI SCRIVI AL DIRETTORE

Accade in Puglia Cronaca Economia Informatica e Hi Tech PRIMO PIANO

Nuovo balzo di attacchi informatici in Italia nei primi mesi dell'anno: il cybercrime colpisce app, social e banking online

6 Maggio 2021 Redazione Oraquadra 0 commenti furto dei dati, Osservatorio Cybersecurity di Exprivia, violazioni della

ULTIMENOTIZIEOGGI

HOME POLITICA CRONACA ECONOMIA LAVORO TECNOLOGIA SPORT GAMING

Exprivia, nuovo balzo cyber attacchi in Italia

6 Maggio 2021

Sono stati 349 da gennaio a marzo 2021, sette volte di più rispetto ai primi tre mesi del 2020. Nel mirino App, social e banking online ...

Italiano | Francese

Région Autonome Vallée d'Aoste — Regione Autonoma Valle d'Aosta

Regione Autonoma Valle d'Aosta

E-mail certificata | Intranet | contatti

LA REGIONE | AREA DI ATTIVITÀ | AL SERVIZIO DEL PUBBLICO | AVVISI E DOCUMENTI | IMPRESE CON PARTECIPAZIONE REGIONALE

Pagina iniziale ▸ Notizie del giorno ▸ Nuovo

Cybersecurity: +47% crimini informatici in Italia nel 2021

ANSA

12:13 - 06/05/2021 Stampa

(ANSA) - BARI, 06 MAG - Nel primo trimestre 2021 in Italia ci sono stati 349 informati, tra attacchi, crimini e crimini della privacy, in crescita del 47% rispetto al 2020. E' quanto emerge nell'ultimo report dell' Osservatorio Cybersecurity di Exprivia. A un anno dallo scoppio della pandemia che portato alla massiccia diffusione dello smart working e al ricorso sempre più frequente a servizi online, l'Osservatorio rileva una forte crescita degli attacchi (+56% rispetto all'ultimo trimestre 2020) ma il numero medio di incidenti, ovvero attacchi andati a buon fine, registra una flessione del 18%.

lunedì, 07 febbraio 2022

Seguici su

IL GIORNALE D'ITALIA

Il Quotidiano Indipendente

Cerca...

"La libertà al singolare esiste solo nelle libertà al plurale" Benedetto Croce

Politica Esteri Cronaca Economia Sostenibilità Innovazione Lavoro Salute Cultura Costume Spettacolo Sport Motori iGdI TV

» Giornale d'italia » Cronaca

Cybercrime: nuovo balzo di attacchi informatici in Italia su app, social e banking online

L'Osservatorio Cybersecurity di Exprivia registra nel primo trimestre dell'anno 349 eventi criminali, in continua crescita rispetto al 2020. Calano i crimini informatici a tema Covid. Il furto dei dati è in cima alla classifica dei danni

06 Maggio 2021

Continua a crescere il trend degli attacchi informatici in Italia anche nel 2021. Da quanto emerge nel primo rapporto del 2021 sulle minacce informatiche in Italia elaborato dall'**Osservatorio Cybersecurity di Exprivia**, nel periodo

THE WORLD NEWS | WORLD NEWS PLATFORM

ITALY TRUSTED 3/5/2021, 15:56:33

Exprivia, nel 2020 crescono indici di redditività malgrado la pandemia

IL DOCUMENTO

Approvati i dati di bilancio. Bene i settori della Sanità e dell'Aerospazio

Exprivia ha approvato i dati 2020 di gruppo, positivi nonostante gli effetti della pandemia con tutti gli indici di redditività che crescono a doppia cifra. In particolare, riferisce una nota, l'azienda registra ricavi in linea con il 2019 che, riflettendo l'andamento dei mercati in cui opera, si attestano a 167,8 milioni rispetto ai 168,5 milioni del 2019. Tutti gli indicatori di marginalità sono positivi: l'EBITDA è in significativo miglioramento attestandosi a 21,4 milioni nel 2020 in incremento del 27,0% rispetto ai 16,8 milioni del 2019, l'EBIT si attesta a 15,0 milioni in incremento del 44,3% rispetto ai 10,4 milioni de 2019, l'EBT a 11,5 milioni in incremento del 74,0% rispetto ai 6,6 milioni del 2019, per arrivare ad un risultato netto pari a 8,6 milioni più che raddoppiato rispetto ai 4,0 milioni del 2019.

NETWORK DIGITAL 360

CYBERSECURITY360

Cyber crime e consapevolezza, importante investire in cultura della sicurezza: ecco perché

Home > Cultura cyber

La pandemia ha contribuito a velocizzare il processo di digitalizzazione: la conseguenza è una distribuzione sempre più uniforme del cyber crime su tutto il territorio italiano e questo ci ricorda che la mancanza di cultura di sicurezza è la vulnerabilità maggiormente sfruttata dagli attaccanti

29 Apr 2021

R **Domenico Raguseo**
Head of CyberSecurity Exprivia

MarketScreener

BORSA | NOTIZIE | ANALISI | CONSIGLI | PORTAFOGLI | ELENCHI | MIGLIORI E PEGGIORI | SCREENERS

Home > Azioni > Italia > Borsa Italiana > Cy4gate S.p.A. > Notizie > Riassunto CY4 IT0005412504

CY4GATE S.P.A. (CY4)

Aggiungere al mio elenco

Tempo differito Borsa Italiana - 07/02 12:40:36

11.02 EUR +0.55%

27/01 **CY4GATE S P A**: menzionata come "Representative Provider" nel rapporto di Gartn... PU
26/01 **CY4GATE**: menzionata come "Representative Provider" in rapporto Gartner DJ
10/01 **CY4GATE S P A**: si è aggiudicata un contratto per primaria istituzione nazionale per ... PU

Riassunto | Quotazioni | Grafici | Notizie | Rating | Agenda | Società | Finanza | Consensus | Revisioni | Derivati

Riassunto | Tutte le notizie | Altre lingue | Comunicati stampa | Pubblicazioni ufficiali | Notizie del settore

Cy4gate: il 28/11 prima Business Partner Conference

12-04-2021 | 12:25

MILANO (MF-DJ)--CY4GATE, società attiva nel mercato cyber a 360*, rende noto che il 28 maggio avrà luogo la prima Business Partner Conference organizzata dalla Società presso la sede di Elettronica Group.

L'evento sarà l'occasione per CY4GATE di condividere con i propri Partner la visione e le tendenze del mercato della Cyber Security e della Decision Augmentation e fornire tutti gli elementi per assicurarsi un business di successo in questi settori in costante crescita e sempre più strategici per le Aziende, dalle PMI alle Corporate.

All'evento saranno presenti, in qualità di Business Partner, società come Engineering, Exprivia, Sielte, Present, Dimira, Cybertech, HTDI, AGATOS Syntagma ed ALFA Group. Per CY4GATE parteciperanno Emanuele Galtieri, Chief Executive Officer, Enrico Fazio, Chief Commercial Officer (CCO), Andrea Pompili, Chief Scientist Officer, e Katia Redini, Enterprise Sales Manager, che illustreranno le novità tecnologiche, condividendo le modalità di proposizione verso il cliente e gli obiettivi, e raccogliendo testimonianze di successo.

alb

alberto.chimenti@mfdowjones.it

(END) Dow Jones Newswires

Dati finanziari EUR

Fatturato 2021	19,0 M	Capitalizzazione	164 M
Risultato netto 2021	4,00 M	VS / Fatturato 2021	8,43x
Liqui. netta 2021	4,30 M	VS / Fatturato 2022	5,37x
P/E ratio 2021	41,5x	N. di dipendenti	69
Rendimento 2021	-	Flottante	-

» Più Dati finanziari

Grafico CY4GATE S.P.A.

Durata : Auto. Periodo : Giorno

» Grafico a schermo intero

AD ANALISIDIFESA

HOME | REDAZIONE E AUTORI | ARTICOLI | SCRIVICI | PUBBLICITÀ | NUMERI PRECEDENTI | SOSTIENICI

CY4GATE annuncia la prima business partner conference

12 aprile 2021 *di Redazione* *in Cyber*

CY4GATE (AIM: CY4) – società attiva nel mercato cyber a 360°, comunica che il 28 maggio avrà luogo la prima Business Partner Conference organizzata dalla Società presso la sede di Elettronica Group.

Fondato e diretto da Luca Tatarelli
Report Difesa
Geopolitica & Sicurezza
Intelligo ergo scribo

Industrie della Difesa

CY4GATE: il 28 maggio avrà luogo la prima Business Partner Conference

DI REDAZIONE PUBBLICATO IL 12 APRILE 2021 NESSUN COMMENTO

Roma. CY4GATE comunica che il 28 maggio avrà luogo la prima Business Partner Conference organizzata dalla Società presso la sede di Elettronica Group.

L'evento sarà l'occasione per CY4GATE di condividere con i propri Partner la visione e le tendenze del mercato della Cyber Security e della Decision Augmentation e fornire tutti gli elementi per assicurarsi un business di successo in questi settori in costante crescita e sempre più strategici per le Aziende, dalle PMI alle Corporate.

il Corriere della Sicurezza
direttore Tiziana Capponi
giornale on line

Aziende news Sicurezza reti Sistemi e aziende

CY4GATE annuncia la prima Business Partner Conference

12 Aprile 2021

redazione

CY4GATE (AIM: CY4) – società attiva nel mercato cyber a 360°, comunica che il 28 maggio avrà luogo la prima Business Partner Conference organizzata dalla Società presso la sede di Elettronica Group.

WIRED SCIENZA ECONOMIA CULTURA GADGET SECURITY DIRITTI IDEE VIDEO PODCAST

REDAZIONE SECURITY 03.04.2021

Torna la più importante conferenza italiana dedicata alla cybersecurity

Dal 7 al 9 aprile online gli appuntamenti dedicati a sicurezza informatica, telecomunicazioni, minacce digitali e nuove forme di protezione

Itasec21 ai nastri di partenza: si terrà dal **7 al 9 aprile** la quinta edizione della **principale conferenza nazionale sulla sicurezza informatica**, per la prima volta interamente online.

BANCAFORTE innovation key Temi Speciali eventi Rubriche Bancaforte

Trend topics Covid-19 Credito PSD2 Fintech Blockchain

SICUREZZA

Cybercrime in crescita nel 2020

di Flavio Padovan - 1 Marzo 2021

Secondo l'Osservatorio Exprivia la pandemia ha causato un aumento dei reati informatici in Italia, con un picco nel mese di dicembre

Secondo le evidenze dell'ultimo rapporto sulle minacce informatiche in Italia elaborato dall'Osservatorio Cybersecurity di Exprivia, nell'ultimo trimestre del 2020 si sono registrati 237 crimini informatici, in aumento del 60% sul trimestre precedente e quasi del 400% rispetto al periodo gennaio-marzo, quando furono solo 49.

CYBERSECURITYITALIA

Itasec21 ai nastri di partenza: si terrà dal 7 al 9 aprile la quinta edizione della principale conferenza nazionale sulla sicurezza informatica, per la prima volta interamente online.

City Roma

CRONACA

Torna la più importante conferenza italiana dedicata alla cybersecurity

3 APRIL 2021

Dal 7 al 9 aprile online gli appuntamenti dedicati a sicurezza informatica, telecomunicazioni, minacce digitali e nuove forme di protezione

Itasec21 ai nastri di partenza: si terrà dal **7 al 9 aprile** la quinta edizione della **principale conferenza nazionale sulla sicurezza informatica**, per la prima volta interamente online.

City Milano

CRONACA

Torna la più importante conferenza italiana dedicata alla cybersecurity

3 APRIL 2021

Dal 7 al 9 aprile online gli appuntamenti dedicati a sicurezza informatica, telecomunicazioni, minacce digitali e nuove forme di protezione

Itasec21 ai nastri di partenza: si terrà dal 7 al 9 aprile la quinta edizione della principale conferenza nazionale sulla sicurezza informatica, per la prima volta interamente online.

MENU | CERCA la Repubblica ABBONATI GEDI SMILE | R

Economia

Truffe via Internet, attenzione all'home banking

Pochi e semplici, ma importanti accorgimenti possono aiutarci a proteggere i nostri risparmi

26 MARZO 2021

Secondo l'Osservatorio Cybersecurity, lo studio sui crimini informatici elaborato da Exprivia, negli ultimi tre mesi del 2020 in Italia sono stati registrati 237 crimini informatici.

Fondato e diretto da Luca Tatarelli

Report Difesa
Geopolitica & Sicurezza
Intelligo ergo scribo

HOME CHI SIAMO EDITORIALI GEOPOLITICA FORZE ARMATE POLIZIA LOCALE POLIZIA DI STATO CARABINIERI ESERCITO
MARINA MILITARE AERONAUTICA MILITARE NEWS MENU MAGAZINE

Intelligence

ITASEC21 Perimetro nazionale, diplomazia cibernetica e sicurezza in orbita: al via la principale conferenza di cybersecurity in Italia

DI REDAZIONE PUBBLICATO IL 3 APRILE 2021 NESSUN COMMENTO

Roma. Itasec21 ai nastri di partenza.

Si terrà dal 7 al 9 aprile la quinta edizione della principale conferenza nazionale sulla sicurezza informatica, per la prima volta interamente online.

DIRETTORE: FILIPPO ASTONE LUNEDÌ 7 FEBBRAIO 2022, 14:35

INDUSTRIA ITALIANA

ANALISI E NEWS SU ECONOMIA REALE, AUTOMAZIONE, INNOVAZIONE, B2B TECH

HOME INDUSTRIA DIGITAL TRANSFORMATION & ICT
AUTOMAZIONE, ROBOT & I.A. ECONOMIA ITALIANA

DIGITAL TRANSFORMATION & ICT

Exprivia entra nella ioXt Alliance, per una maggiore sicurezza dei dispositivi connessi

Il team cybersecurity dell'azienda verificherà l'adozione di protocolli crittografici affidabili e verificherà le vulnerabilità dei software e il loro processo di aggiornamento

25 Marzo 2021

MarketScreener

BORSA | NOTIZIE | ANALISI | CONSIGLI | PORTAFOGLI | ELENCHI | MIGLIORI E PEGGIORI | SCREENERS

Home > Azioni > Italia > Borsa Italiana > Exprivia S.p.A. > Notizie > Riassunto XPR IT0001477402

EXPRIVIA S.P.A. (XPR)

Tempo reale stimato Cboe Europe - 07/02 14:26:30

2.115 EUR **+0.24%**

03/02 **EXPRIVIA S P A**: Borsa Italiana - Il calendario 2022 degli eventi societari di Exprivia
03/02 **DATA MANAGER - PARKINSON**: un robot per la terapia dei pazienti a ritmo di danz...
01/02 **EXPRIVIA S P A**: Corriere della sera - Curare il Parkinson con le danze irlandesi. E i...

Riassunto | Quotazioni | Grafici | **Notizie** | Rating | Agenda | Società | Finanza | Consensus | Revisioni | Derivati

Riassunto | Tutte le notizie | Altre lingue | Comunicati stampa | Pubblicazioni ufficiali | Notizie del settore

Exprivia aderisce a ioXt Alliance: più sicurezza per i dispositivi connessi in rete

25-03-2021 | 11:05

EXPRIVIA ADERISCE A IOXT ALLIANCE: PIÙ SICUREZZA PER I

DISPOSITIVI CONNESSI IN RETE

Tra le prime società italiane a entrare nel network globale di ioXt Alliance, da oggi Exprivia potrà fornire nuovi servizi per certificare la sicurezza dei dispositivi IoT riducendo il rischio di attacchi criminali.

25 marzo 2021-Expriviaè diventata membro diioXt Alliance(Internet of secure things), il network globale per la sicurezza dei dispositivi IoT che coinvolge i principali attori del settore tecnologico conl'obiettivo dicreare standard di sicurezza riconosciuti e applicati a livello internazionale.

Exprivia è trale prime società italiane ad entrare nell'Alliance con la qualifica di Affiliate,diventando un punto di riferimento per le società italiane che intendono certificare la sicurezza dei propri dispositivi connessi in rete. Il team CyberSecurity verificherà l'adozione diprotocolli crittografici affidabili, con meccanismi di autenticazione che non consentano password universali, e verificherà le vulnerabilità dei software e il loro processo di aggiornamento per tutelare la sicurezza in un lasso di tempo minimo garantito.

Dati finanziari EUR

Fatturato 2021	175 M	Capitalizzazione	
Risultato netto 2021	-	VS / Fatturato 2021	
Indebitamento netto 2021	34,0 M	VS / Fatturato 2022	
		N. di dipendenti	
P/E ratio 2021	12,3x	Flottante	
Rendimento 2021	-		

» Più Dati finanziari

Grafico EXPRIVIA S.P.A.

Durata : Auto. Periodo : Giorno

8 ott 2021 - 7 feb 2022 - Ultimo : 2,11

MA(20) 2,08 MA(50) 2,14 MA(100) 2,07

BitMAT | BitMATv | Top Trade | Linea EDP | Itis Magazine | Speciale Sicurezza | Industry 4.0 | Sanità Digitale | Redazione

BitMAT

NEWS | INTERNET | SICUREZZA | CASE HISTORY | TECNOLOGIE | MERCATO | VERTICAL

Hacker Field: il cyber game Hacker vs IT manager

Da **Redazione BitMAT** - 23/03/2021

Il Cyber Game "Hacker Field" diverte con la sicurezza informatica e permette agli utenti di sfidarsi in due ruoli: hacker o IT manager

NETWORK DIGITAL 360

CORCOM

STRATEGIE

Exprivia entra nell'ioXt Alliance e spinge sulla sicurezza dei dispositivi connessi

Home > Cyber Security

Tra le prime realtà italiane nel network globale con la qualifica di Affiliate, l'azienda punta a diventare un punto di riferimento per la certificazione. Raguseo: "Fondamentali gli standard globalmente riconosciuti"

25 Mar 2021

MENU CERCA IL MATTINO.it

NAPOLI AVELLINO BENEVENTO SALERNO CASERTA CALABRIA

HOME PRIMO PIANO ECONOMIA CULTURA SPETTACOLI SPORT TECNOLOGIA

HITECH APPLE SAMSUNG SMARTPHONE TABLET APP-GIOCHI TV-FOTO SCIENZA INTERNET MOLTOFUTURO

Cyber Game, nei panni dell'hacker per difendersi in rete

TECNOLOGIA > APP E GIOCHI

Martedì 23 Marzo 2021

La pandemia ha aumentato gli attacchi informatici in Italia, cresciuti del 250% nel secondo trimestre del 2020 (dati osservatorio cybersecurity Exprivia).

WIRED

Torna la più importante conferenza italiana sulla sicurezza informatica

Dal 7 al 9 aprile si terrà la quinta edizione di Itasec, per la prima volta gratuita e online, riunisce ricercatori e professionisti dal mondo accademico, industriale e governativo

Dal 7 al 9 aprile si terrà la quinta edizione di ITASEC: principale conferenza nazionale sulla sicurezza informatica. Organizzato dal Laboratorio Nazionale di Cybersecurity del CINI (Consorzio Interuniversitario Nazionale per l'Informatica) e di cui *Wired* è media partner, l'evento, per la prima volta gratuito e interamente online, riunisce ricercatori e professionisti provenienti dal mondo accademico, industriale e governativo per discutere delle sfide emergenti e dei bisogni consolidati nel campo della cybersecurity.

ANSA.it Press Release

Fai la ricerca | ABBONATI | Accedi o Registrati

Cronaca | Politica | Economia | Regioni + | Mondo | Cultura | Tecnologia | Sport | FOTO | VIDEO | Tutte le sezioni +

SPECIALI Ambiente • ANSA2030 • ANSA ViaggiArt • Eccellenze • Expo Dubai • Industry 4.0 • Legalità • Lifestyle • Mare • Motori • Salute • Scienza • Terra&Gusto

COMUNICATO STAMPA - Responsabilità editoriale PANDANT

Cyber Game, nei panni dell'hacker per difendersi in rete

"Hacker Field" diverte con la sicurezza informatica: sviluppato da un team italiano a Londra, permette agli utenti di sfidarsi in due ruoli, come hacker o IT manager

PANDANT 22 marzo 2021 10:51

La pandemia ha aumentato gli **attacchi informatici in Italia**, cresciuti del 250% nel secondo trimestre del 2020 (dati osservatorio cybersecurity Exprivia). La sicurezza informatica è un tema sempre più decisivo per il futuro e gli attacchi informatici sono stati inseriti tra le dieci minacce peggiori per il mondo nel report annuale del World Economic Forum, **"The Global Risks Report 2020"**:

affaritaliani.it 25 ANNI ONLINE DAL 1996

Il primo quotidiano digitale, dal 1996

Conte | Coronavirus | Meteo ATTIVA LE NOTIFICHE | FONDATORE E DIRETTORE: ANGELO MARIA PERRINO

Home > Mediatech >Cyber Game, arriva il gioco nei panni dell'hacker per difendersi in rete

MEDIATECH A- A+

Lunedì, 22 marzo 2021 - 13:11:00

Cyber Game, arriva il gioco nei panni dell'hacker per difendersi in rete

Dell'imprenditore italiano Antonio Gison l'app per imparare come comportarsi in un attacco informatico. Partita una campagna di crowdfunding su Kickstarter

Eduardo Cagnazzi

La pandemia ha aumentato gli attacchi informatici in Italia, cresciuti del 250% nel secondo trimestre del 2020 (dati osservatorio cybersecurity Exprivia).

ASSINEWS.it
il quotidiano assicurativo

HOME NEWS RIVISTA TECNICA E NORME MERCATO NEWSLETTER ANNUNCI ESPERTORISPONDE ABBONATI!

Home › Tecnica assicurativa › Assicurazione Danni › Cyber attacchi, un anno nero Covid e vaccini fanno da esca

Cyber attacchi, un anno nero Covid e vaccini fanno da esca

8 Marzo 2021

Lo scenario relativo al 2020 delineato da Clusit, F5 Labs, CyberArk, Fortinet ed Exprivia

Pagine a cura di Antonio Longo

In piena pandemia sono aumentati del 12% gli attacchi informatici nel mondo, il 10% ha sfruttato il tema «Covid-19», tanto che nel mirino degli hacker è finito anche lo sviluppo dei vaccini.

BitMAT BitMATv Top Trade Linea EDP Itis Magazine Speciale Sicurezza Industry 4.0 Sanità Digitale Redazione

BitMAT

NEWS INTERNET SICUREZZA CASE HISTORY TECNOLOGIE MERCATO VERTICAL APP

Home › Portale BitMat › Portale Evidenza

Cybercrime: è dicembre il mese peggiore del 2020

Da **Redazione BitMAT** - 02/03/2021

Vola il Cybercrime: l'Osservatorio Cybersecurity di Exprivia registra, nell'ultimo trimestre dell'anno, una crescita dei reati informatici. Quasi cinque volte superiore rispetto al primo

Fondato e diretto da Luca Tatarelli
Report Difesa
Geopolitica & Sicurezza
Intelligo ergo scribo

Sicurezza nazionale

Sicurezza informatica: dal 7 al 9 aprile la quinta edizione di "ITASEC"

DI REDAZIONE PUBBLICATO IL 11 MARZO 2021 NESSUN COMMENTO

Roma. Si terrà dal 7 al 9 aprile la quinta edizione di "ITASEC", la principale Conferenza nazionale sulla sicurezza informatica.

CORRIERE DELLA SERA
CORRIERE DEL MEZZOGIORNO / CRONACA

LA RILEVAZIONE

Il cybercrime scommette sulla sanità «Attenti ai dati sensibili sul web»

L'osservatorio Cybersecurity di Exprivia mette in guardia il popolo di internet dalle truffe. «Crescono del 300% delle violazioni di sicurezza dopo il primo trimestre 2020»

NETWORK DIGITAL 360

CORCOM

Digital Economy Telco Industria 4.0 PA Digitale Space economy

SCENARI

Cybercrime, per l'Italia si mette male: sempre più nel mirino pagamenti cashless e sanità

Home > Cyber Security

L'Osservatorio sulla cybersecurity di Exprivia registra nell'ultimo trimestre 2020 una crescita del 400% dei reati informatici. Tra le tecniche più utilizzate l'adescamento tramite e-mail e social network

key4biz

YBERSECURITY » REPORT EXPRIVIA SULLA CYBERSECURITY: CRESCONO I REATI IN ITALIA. NEL MIRINO PA E SANITÀ

LO STUDIO

Report Exprivia sulla cybersecurity: crescono i reati in Italia. Nel mirino PA e sanità

di **Flavio Fabbri** | 24 Febbraio 2021, ore 15:59

Osservatorio Cybersecurity di Exprivia: dicembre si conferma il mese peggiore del 2020 in Italia per la sicurezza in rete. PA e finanza tra i settori più colpiti, quest'ultima soprattutto per l'incremento dei pagamenti cashless. Primeggia l'adescamento tramite email e social network. Presi di mira i dispositivi medicali.

I cyber criminali non vanno in vacanza, non dormono e non si ammalano, sono sempre in agguato dietro ad ogni mail che ci arriva, ad ogni device connesso in rete, ad ogni transazione finanziaria e dietro ad ogni acquisto di prodotto o servizio.

L'autore

Flavio Fabbri

FIRST online

Presidente: Ernesto Auci Direttore: Franco Locatelli

ECONOMIA E IMPRESE · FINANZA E MERCATI · RISPARMIO · PENSIONI · TASSE · LAVORO · FOOD · CULTURA · SPORT · POLITICA · MONDO

NEWS INTERVISTE COMMENTI ARTE TECH TUTORIAL TUTTE LE NOTIZIE COMPARA TARIFFE FACEBOOK TWITTER LINKEDIN RSS

HOME ▸ TECH ▸ CYBERCRIME, DICEMBRE 2020 MESE NERO PER GLI ATTACCHI INFORMATICI

Cybercrime, dicembre 2020 mese nero per gli attacchi informatici

7 Marzo 2021, 12:44 | di Redazione FIRSTonline

Il mese peggiore del 2020 per i crimini informatici è stato Dicembre; è quanto emerge dall'ultimo rapporto sulle minacce informatiche dell'Osservatorio Cybersecurity di Exprivia, dove si registra, nell'ultimo trimestre dell'anno, una crescita dei reati informatici. Tra i settori più colpiti? La finanza, a causa dell'aumento dei pagamenti cash-less e i dispositivi medicali

SICUREZZA.net Esperti in Cybersecurity

CYBER SECURITY

Cyber Security: crescono i reati in Italia

Anna Ercoli 26 Febbraio 2021

Secondo il rapporto **Exprivia**, i crimini di cyber security in Italia sono in aumento. I settori maggiormente colpiti sono la **finanza** e la **pubblica amministrazione**.

DMO Data Manager Online il portale dell'ICT professionale

SOFTWARE HARDWARE WEB E SOCIAL MERCATO IT TOP100 WHITE PAPERS #WECHANGEIT

Software Sicurezza

Cybercrime: è dicembre il mese peggiore del 2020

Di **Redazione Data Manager Online** - 24 Febbraio 2021

L'Osservatorio Cybersecurity di Exprivia registra nell'ultimo trimestre dell'anno una crescita dei reati informatici quasi cinque volte superiore rispetto al primo

Dopo mesi altalenanti, tornano a crescere a fine anno i **reati informatici in Italia**; con un picco a dicembre, il 2020 si conferma un anno complesso anche per quanto concerne la sicurezza in rete.

Borderline 24 - Il giornale -

PRIMA PAGINA | BARI | ATTUALITÀ | CRONACA | CULTURA | ECONOMIA | POLITICA | ISTRUZIONE | SPORT

Nazionale

Crimini informatici, in pandemia aumento del 300%: rapporto dell'osservatorio Exprivia

Di **redazione** - 24 Febbraio, 2021

Le informazioni sullo stato di salute dei pazienti sono una notevole fonte di guadagno per gli hacker: per questo motivo la sanità rappresenta uno dei settori più "attrattivi" per il cybercrime, con un aumento pari al 300% delle violazioni di sicurezza dopo il primo trimestre 2020.

Search

CYBERSECURITYITALIA

Home | Italia | Europa | Mondo | Homeland Security | Report | Eventi | Video

Report Exprivia: cyber reati in aumento in Italia. Colpiti PA, finanza e sanità

FLAVIO FABBRI — 24 FEBBRAIO 2021 — ITALIA

L'Osservatorio Cybersecurity di Exprivia ha registrato nell'ultimo trimestre una crescita dei reati informatici cinque volte superiore rispetto all'inizio del 2020. PA e finanza tra i settori più colpiti. Gli obiettivi principali furto dati e violazione privacy. Presi di mira dai cyber criminali anche le strutture sanitarie.

I cyber criminali non vanno in vacanza, non dormono e non si ammalano, sono sempre in agguato dietro ad ogni mail che ci arriva, ad ogni device connesso in rete, ad ogni transazione finanziaria e dietro ad ogni acquisto di prodotto o servizio.

IL GIORNALE DELLE PMI

CRESCIMPRESA | INFOIMPRESA | INNOVAZIONE | EXPORT IN DIGITALE | INTERNAZIONALIZZAZIONE | INTERVISTE | TECNOLOGIA

Home > La rassegna dell'una > Cybercrime: è dicembre...

Cybercrime: è dicembre il mese peggiore del 2020

LA RASSEGNA DELL'UNA TECNOLOGIA

Redazione 25 Febbraio 2021

Dopo mesi altalenanti, tornano a crescere a fine anno i **reati informatici in Italia**; con un picco a dicembre, il 2020 si conferma un anno complesso anche per quanto concerne la sicurezza in rete.

Da quanto emerge nell'ultimo **rapporto del 2020 sulle minacce informatiche** **in Italia** elaborato dall'**Osservatorio Cybersecurity di Exprivia**, nel periodo **ottobre-dicembre** si sono registrati 237 crimini informatici, in crescita del 60% sul trimestre precedente e quasi del 400% rispetto al periodo gennaio-marzo, quando furono solo 49.

ICT Security MAGAZINE

Home | Articoli | Rubriche | Notizie | Eventi | Newsletter

Migrare verso il cloud in sicurezza

A cura di: Domenico Raguseo - Pubblicato il 15 Febbraio 2021

La scelta di un modello di business e di delivery flessibile e dinamico come quello del cloud è oramai diventata imprescindibile. Il cloud, infatti, rappresenta il modo migliore per poter indirizzare le necessità di scalabilità e ottimizzazione di risorse necessarie per garantire e supportare la crescita delle aziende. Allo stesso tempo però le direttive sulla privacy e il cybercrime suggeriscono che la sicurezza debba essere un elemento di discussione se si decide di migrare i servizi verso il cloud.

MENU | CERCA

la Repubblica

Economia&Finanza

HOME MACROECONOMIA FINANZA LAVORO DIRITTI E CONSUMI AFFARI&FINANZA OSSERVA ITALIA CALCOLATORI GLOSSARIO LISTINO PORTAFOGLIO

A&F **MONDO 5G**
Come cambierà la nostra vita con la rete mobile 5G. Le opportunità per famiglie e imprese: più connettività, realtà aumentata e milioni di "cose" connesse. Perché l'Internet of Things rivoluzionerà il nostro quotidiano.

HOME | RETE PER L'ITALIA | INDUSTRY 4.0 | TREND | DIGITAL EDUCATION | STORIE | ARCHIVIO | Cerca nel sito | CERCA

Cybercrimini, 2020 anno nero: sotto attacco sanità, pagamenti cashless e aziende

Il nuovo studio dell'Osservatorio Cybersecurity, elaborato da Exprivia, ha scattato una fotografia che fa preoccupare anche per l'anno appena iniziato. Ecco le tecniche usate dai cybercriminali

di Andrea Frollà

24 Febbraio 2021

Furto dei dati, violazione della privacy e perdite di denaro, dalla pubblica amministrazione alla finanza passando per la sanità. Se il 2020 è stato un annus horribilis per l'intero pianeta a causa della pandemia, non è certo andata meglio nel mondo della **sicurezza informatica** a causa degli effetti collaterali della pandemia stessa. Tra la migrazione forzata del lavoro nelle case e l'emergenza vissuta negli ospedali, i criminali informatici hanno infatti avuto la vita più facile del solito. E a tendere il rischio è che, in **assenza di contromisure adeguate**, la forbice tra attacco e difesa possa allargarsi ulteriormente.

MONDO 5G
Un'iniziativa di Affari & Finanza
in collaborazione con Tim e l'Università Federico II di Napoli

A&F TIM Università degli Studi di Napoli Federico II

A&F **AFFARI&FINANZA**

A cura di
Luigi Gia, Paola Jadeluca e Stefano Carli

Hanno collaborato
Stefania Aoi, Vito de Ceglia, Luigi Dell'Olio, Silvano Di Meo, Sibilla Di Palma, Andrea Frollà, Marco Frojo, Valerio Gualerzi, Mariano Mangia, Raffaele Ricciardi

BitMAT

NEWS INTERNET SICUREZZA CASE HISTORY TECNOLOGIE MERCATO VERTICAL APP

Home › News

La Giornata della protezione dei dati, meglio conosciuta come Data Privacy Day

Da **Redazione BitMAT** - 25/01/2021

Quando e perchè è nata la Giornata della protezione dei dati?

I dati personali di ciascuno di noi vengono elaborati ogni secondo fornendo informazioni sulle nostre abitudini, stili di vita, relazioni personali, stato di salute e situazione finanziaria.

EXPRIVIA S.P.A. (XPR)

Aggiungere al mio elenco

Tempo reale stimato Cboe Europe - 07/02 14:51:31

2.135 EUR **+1.18%**

03/02 **EXPRIVIA S P A**: Borsa Italiana - Il calendario 2022 degli eventi societari di Exprivia PU
03/02 **DATA MANAGER - PARKINSON**: un robot per la terapia dei pazienti a ritmo di danz... PU
01/02 **EXPRIVIA S P A**: Corriere della sera - Curare il Parkinson con le danze irlandesi. E i... PU

Cybercrime : dicembre il mese peggiore del 2020

24-02-2021 | 18:03

MILANO (MF-DJ)--Nel periodo ottobre-dicembre si sono registrati 237 crimini informatici, in crescita del 60% sul trimestre precedente e quasi del 400% rispetto al periodo gennaio-marzo, quando furono solo 49.

È quanto emerge nell'ultimo rapporto del 2020 sulle minacce informatiche in Italia elaborato dall'Osservatorio Cybersecurity di Exprivia.

È marzo il mese che segna lo spartiacque nella dinamica del cybercrime: con l'inizio della pandemia e, con essa, della diffusione dello smart working, si legge in una nota, si è assistito a un'impennata tra attacchi informatici, violazioni della privacy e incidenti in tutti i settori dell'economia e della pubblica amministrazione.

In tutto il 2020, oltre il 60% degli eventi criminali ha provocato il furto dei dati, superando di gran lunga sia le violazioni della privacy (13% dei casi) - quasi triplicate dall'inizio dell'anno - che le perdite di denaro (10%). Nel 2020 la Pubblica Amministrazione e il settore Finance sono stati gli ambiti maggiormente attaccati dai cybercriminali, a seguire il settore Education, preso di mira a causa del massiccio ricorso alla didattica a distanza di scuole e università. Non è da meno il settore dell'Industria che dopo aver registrato picchi incrementali durante tutto l'anno, conta solo nell'ultimo trimestre 17 eventi criminali, quasi il 50% dell'intero 2020, causati da una crescita di dispositivi collegati alla rete, molti privi di autenticazione, e anche da tanti episodi di spionaggio industriale.

Dati finanziari EUR

Fatturato 2021	175 M	Capitalizzazione	99,9 M
Risultato netto 2021	-	VS / Fatturato 2021	0,76x
Indebitamento netto 2021	34,0 M	VS / Fatturato 2022	0,67x
P/E ratio 2021	12,3x	N. di dipendenti	-
Rendimento 2021	-	Flottante	-

» Più Dati finanziari

Grafico EXPRIVIA S.P.A.

Durata : Auto. Periodo : Giorno

» Grafico a schermo intero

Importanza della consapevolezza

Phishing attacks:
AN EASY AND VERY DANGEROUS TECHNIQUE

Phishing 2020 continues to be the preferred attack technique by cybercriminals. According to Exprivia Threat Intelligence Report 3Q2020, in the 3rd quarter of 2020, 62 phishing campaigns were analysed in Italy with a total of 138 since the beginning of 2020. Industries most impacted are Finance, Healthcare, Industry and Public Administration. Phishing begins with an email or other fraudulent communication sent for the purpose of attracting a victim. The message appears to come from a reliable sender. If the deception is successful, the victim is urged to provide confidential information, often on a scam website. Sometimes, malware is also downloaded to the victim's computer. Sometimes it is enough for hackers to obtain victim's credit card information or other personal data for profit. Other times, phishing emails are sent to obtain employee login credentials or other information to perform a more sophisticated attack against a specific company.

Cyber-attacks such as persistent advanced threats (APT) and ransomware often begin with phishing. One of the most important way to protect an organisation from phishing is to increase the awareness and the culture of cybersecurity. Education should involve all employees. Senior executives are often the target of phishing campaign. Exprivia provides a large catalogue of courses with the aim of improving awareness and competence to reduce the risk of a Cybersecurity incident and limit the consequent damages.

Millions of interconnected IoT devices:
HOW TO FACE SECURITY?

The Internet of Things is surrounding us with an ever-increasing number of IoT devices that can control industrial processes or common activities. Having those devices connected through the network make them vulnerable to external attacks. For this reason, it is strongly recommended to secure devices as they can be the entry point for compromising the service directly connected at the device. Protecting the IoT device is not helping just to be more secure, but helps to keep the entire ecosystem more secure. With regards to cybersecurity, with IoT it is clear that investment cannot be done just to secure the service, we need to invest to keep the entire ecosystem more secure. This is not a trivial difference in a world where investments are done based on ROI. In fact, it is not unusual to find, on the network, devices with default credentials or with missed security protocols which represent an easy attack surface (more information here).

An analyis by Exprivia's CyberSecurity Observatory in 2020 identified about 476M of interconnected devices on the planet. These devices include: cameras, routers, firewalls, smartTVs, printers, thermostats, medical devices and several other smart devices including PLC controlling industrial system (full analysis and graphs are available here).

Exprivia is committed to improving awareness on IoT security, researching vulnerabilities, participating in committees related to new protocols and helping customers to enable IoT devices in a secure way.

If you want to learn more about IoT, check out this course from Exprivia.

MALWARE: A NEVER STOPPED EVOLUTION

Since the Zeus source code was made public in 2011, the history of malware has changed. In fact, the availability of the source code opened the doors for the creation of a number of new, updated versions of the malware. Therefore, while the original Zeus malware was neutralised, several of its components were used in a large number of new and emerging malware. It is curious that while Zeus has been one of the most malicious malware in the history of humanity, it is mainly known as its source code became public at a certain point, and this has driven a new generation of malware customised by industry (actually many are created for finance and adapted to other industries), type (botnet, trojan, crypto-miners, rootkits, spyware, worms ...), delivery models (for example Citadel is a toolkit to deliver malware but in general gangs are specialised to support specific phases of the kill chain) and by technology (fileless malware for example are activated using software and applications that are already built in the operating system). All the variants with the capability to move, replicate, distribute and hide themselves for years. It is clear that detecting and removing a malware and responding to an attack performed with a malware requires extreme competence and capability to analyse immediately, on the endpoint, a wide amount of data and perform anomaly detection. We could therefore affirm that if virus is evolving to malware, antivirus is evolving to Endpoint Detection and Response technologies.

Exprivia provides a large catalogue of services that can help you manage your approach to cybersecurity.

KEEP UP TO DATE YOUR SECURITY CONTROLS AND DO NOT BECOME A HOSTAGE OF RANSOMWARE!

Ransomware is an attack in which the attacker restricts access to the victim's service (or device), asking for a ransom to return access. The attack can be successful by hooking authentication systems, simply changing the password or encrypting data (like CryptoLocker does). The "ransom" to pay to the cybercriminals, usually is through a hard-to-trace electronic payment method, such as cryptocurrency.

Ransomware is almost always distributed through spam attacks. The spam email contains an attachment disguised as a legitimate file or includes a URL link in the message text.

To activate the payload, most ransomware requires user action. Educating employees to recognise and defend against cyber-attacks is essential.

According to Exprivia's CyberSecurity Observatory, 4Q2020 recorded an increase in ransomware attacks in the Italian perimeter. In particular, there was an increase of 50% compared to 3Q2020 and of 650% compared to the value recorded in 1Q2020. If you want to better understand this trend you can download the Exprivia Threat Intelligence Report here.

Exprivia considers training on awareness and skills in general as a fundamental security control. Consult our awareness program here.

THIS SUMMER COME AND ATTEND THE SECOND EDITION OF THE EXPRIVIA CYBERSECURITY ACADEMY!

Although the attack techniques are increasingly sophisticated and criminals are more determined, as highlighted in the report prepared by the CyberSecurity Observatory of Exprivia (free here), the most used attack technique since the beginning of 2021 is phishing/social engineering.
Therefore, on the one hand it is important to invest in Cybersecurity Awareness (Exprivia boasts an extensive catalogue of courses through Udemy, and other learning channels), on the other hand the CyberSecurity market needs security specialists.
Exprivia, for this reason, has decided to found the Exprivia CyberSecurity Academy, a training path dedicated to young people who want to turn their passion for CyberSecurity into work. This Summer, the second edition of the Exprivia CyberSecurity Academy will start, a real school dedicated to CyberSecurity with the aim of developing the talent and improving the skills of the participants in the programme by providing them with a solid basic preparation in the field of cybersecurity, support from specialists expert in the field and open badge 2.0 certifications on the most used tools in the CyberSecurity world.

BRING YOUR OWN DEVICE WE WILL MANAGE THE SECURITY

The acronym BYOD stands for "Bring Your Own Device" that is the approach to the use of personal devices in public or private business environments. As users potentially mix their personal and professional lives on their devices, they can unintentionally expose their company to destructive cyber-attacks.
The security risks of BYOD are mainly related to data protection so all the measures and the policies to implement will be related to clearly separate the work tasks from the personal tasks, leveraging on the capabilities of the devices and adopting technical solutions like the MDM tools (Mobile Device Management) that allow to implement and manage these policies, managing exceptions and violations.
Almost the same challenges are to be faced by permitting personal use of corporate devices: a clear and well understanding policy has to be adopted, and an MDM tool has to be implemented to manage and monitor the device.
With the same MDM technology, it will also be possible to manage access to the enterprise resources in intranet, configuring Wi-Fi and VPN, leveraging on the existing digital identity and credentials, distribute apps and remove any access or wipe the device in case of loss or stole.
To prevent these risks and improve security posture in the device environment,

SECURE REMOTE WORKING

Today, remote working is widely adopted by many companies for several reasons, therefore, it is necessary to have a safe and secure remote working system. The workstation must be equipped with anti-virus and anti-malware (XDR) technologies and protected with disk encrypting in case of theft or loss while in mobility. The connection used by the worker to connect with the information system is based on standard internet providers and can be protected using different technologies: from the very traditional VPN and access to internally managed Virtual Desktop Interfaces (VDI), to more innovative tools that allow a complete segregation of remote systems, the corporate infrastructure and an approach more compliant with the ZeroTrust paradigm.

Another important security factor that must be implemented to avoid identity theft is the implementation of MultiFactor Authentication (MFA) solutions. Extreme attention must be paid to the implementation of the various security measures that must not be excessively heavy for the operation, because an excess in this direction could lead workers to behaviors opposite to what is desired.

Find out about Exprivia CyberSecurity, which provides various technological solutions for remote working.

CYBERSECURITY 2022

The data observed by the Exprivia Cybersecurity Researchers are suggesting that the fork between attacks and incidents is reducing. This is due to the fact that attackers are always more efficient but also depending on the acceleration of the digitalisation process due to the pandemic. The result of this acceleration has enlarged the perimeter of a possible attacks even if we do not have to consider just the physical perimeter. The perimeter is the set of people, infrastructures and devices connected and collaborating in the digital ecosystem. If the digitalisation process has naturally impacted the number of devices and connections, it has also impacted the number of people using the digital ecosystem, not all of them really ready for the transformation. The paradox is therefore that if on one hand phishing is becoming more sophisticated, the victims on the other hand are less prepared to detect and identify a phishing campaign. Therefore, in 2022, we'll see attackers committed and motivated in using all the vulnerabilities in the enlarged perimeter (including the human vulnerabilities) while in cybersecurity we are requested in the development of the most efficient firewall (human) with awareness programs.

Photoreport

ITASEC 2020

Apulia CyberSecurity 2020

MAM 2021

Apulia CyberSecurity 2021

MAM 2021

MAM 2021

MAM 2021

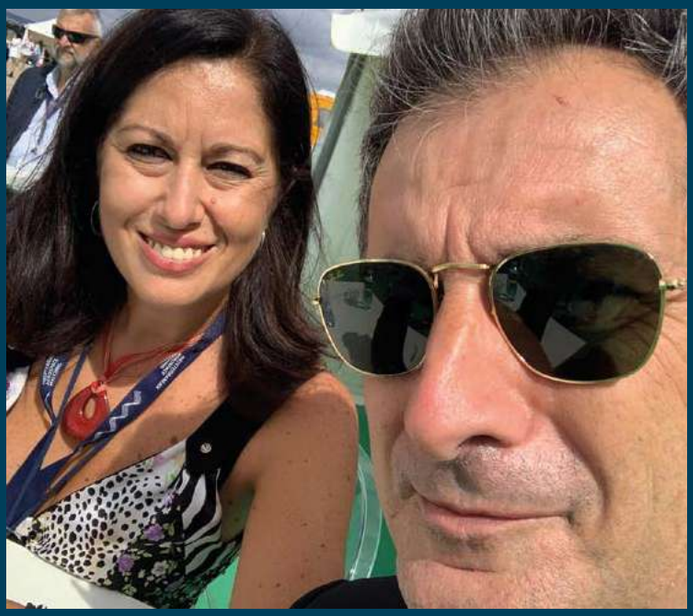
MAM 2021

MAM 2021

MAM 2021

MAM 2021

MAM 2021



MAM 2021

MAM 2021

MAM 2021

MAM 2021

MAM 2021

MAM 2021

MAM 2021

MAM 2021

MAM 2021

MAM 2021

MAM 2021