
Cyber Security
il valore del tuoi dati
CM planet
Progettiamo soluzioni

L'ALLARME

Cyber-spionaggio, Venezuela sotto attacco hacker

Secondo gli analisti di Eset è in atto una campagna che ha per obiettivi le forze armate di diversi Paesi latinoamericani, e in particolare quelle di Caracas. L'iniziativa, denominata "Machete", punta ai file che descrivono le rotte di navigazione e il posizionamento delle unità militari

Medicina e cyberspionaggio, il parere di FireEye

Luke McNamara, Principal Analyst di FireEye, spiega perché i ricercatori nel settore medico sono diventati un obiettivo del cyberspionaggio cinese.

11 Settembre 2019

Aziende sotto scacco e truffe. È allarme cyberspionaggio

Ruben Razzante
Docente di Diritto dell'Informazione

IL BLOG

La cybersecurity è una priorità non più rimandabile

"Spioni" informatici, cyberattacchi durante le elezioni, violazioni della privacy e pubblicazioni di segreti di Stato. La speranza è che si lavori seriamente dotando le nostre forze di polizia e di intelligence di strumenti più adeguati alle sfide che provengono dal mondo del cybercrime. Che sia necessaria un'unica struttura in grado di gestire le emergenze di cybersicurezza ce lo dice anche l'Europa: entro il 2018 anche l'Italia dovrà attuare una direttiva in questo senso.

Cyberspionaggio: scatta il blitz di polizia e Fbi

Ogni azienda, sia essa pubblica o privata, è costantemente minacciata da crimini informatici ed atti di terrorismo cibernetico: dalla creazione di siti per il phishing, al furto di dati ed identità personali, all'introduzione di virus e malware nei sistemi aziendali.

Le conseguenze di tali attacchi possono essere estremamente gravi e causare danni ingenti al business e al brand di una società.

Tra le principali ripercussioni del Cyber Crime, le aziende o imprese pubbliche possono trovarsi a dover affrontare:

- Perdita di informazioni critiche
- Interruzione dei processi di business
- Danni significativi all'immagine dell'azienda
- Danneggiamenti alle infrastrutture nazionali e/o di sicurezza

I numeri del Cyber Crime

Secondo il **Rapporto Clusit sulla sicurezza ICT** sono stati 1.127 gli attacchi “gravi” registrati ed analizzati nel 2017, una crescita del 7% degli attacchi informatici rispetto al 2016.

In Italia nel 2018 danni per **10 miliardi** di €.

Entro il **2021** i danni raggiungeranno quota **6 trilioni di dollari**, una cifra che supera i danni dai traffici di droga mondiali.

Cos’è la Cyber Security?

La **Cyber Security** è l'insieme di tutte le tecniche, mezzi e tecnologie che consentono di proteggere un sistema informatico da attacchi malevoli provenienti dall'esterno, mirati a sottrarre dati e informazioni o a compromettere il funzionamento del sistema stesso.

La posta in gioco, per quanto attiene il tema della Cyber Security, è davvero alta perché coinvolge interessi di persone e aziende, di privati ed enti pubblici, di imprese e professionisti.

Direttiva NIS (Network and Information Security) d.lgs. 65/18

Controlli Essenziali di Cyber Security

- Inventario dispositivi e software
- Governance
- Protezione da Malware
- Gestione Password e Account

- Inventario dispositivi e software
- Protezione dei dati
- Protezione delle reti
- Prevenzione e mitigazione

Inventario dispositivi e software

- Creare inventari di sistemi, dispositivi, software, servizi
- Minimizzare l'esposizione sui social/servizi
- Creare inventari di informazioni, dati e sistemi critici
- Nominare un referente per la Cybersecurity

Gestione Password e Account

- Utilizzare password lunghe e diverse per ogni account, dismissione vecchi account, autenticazione forte
- Effettuare l'accesso ai sistemi usando utenze personali, non condivise con altri
- Applicare il principio del privilegio minimo di accesso alle risorse

Governance

- Identificare e rispettare le leggi e i regolamenti relativi alla Cybersecurity

Formazione e Consapevolezza

- Identificare e rispettare le leggi e i regolamenti relativi alla Cybersecurity

Protezione delle reti

- Utilizzare dispositivi per la protezione delle reti

Protezione dei dati

- Effettuare la configurazione iniziale dei dispositivi tramite esperti
- Definire procedure di backup dei dati critici

Prevenzione e mitigazione

- In caso di incedente informare i responsabili.
  Il ripristino viene curato da personale esperto
- Eseguire gli aggiornamenti software/firmware e dismettere hardware e software non più supportato.

Protezione da Malware

- Utilizzare e mantenere aggiornato software antimalware su tutti i dispositivi che lo consentono

Vulnerability Assessment e Penetration Test

Una corretta gestione della sicurezza si basa innanzitutto su un'adeguata conoscenza dell'attuale livello di protezione dei propri sistemi. Partendo da questo presupposto, CM Planet ha consolidato la propria esperienza nell'applicazione di metodologie di **Vulnerability Assessment** e **Penetration Testing** internazionalmente riconosciute, approcciando il problema da diversi possibili punti di vista ed arrivando rispondere a tutte le esigenze poste dai Clienti in questi ambiti.

Le attività di Vulnerability Assessment e Penetration Test offerte da CM Planet hanno il comune obiettivo di fornire al cliente una conoscenza dettagliata sullo stato di sicurezza dei propri sistemi informatici e due tecniche si differenziano tanto per i risultati che permettono di raggiungere quanto per le risorse necessarie alla loro conduzione.

Come agire?

CM Planet supporta aziende ed organizzazioni nella **gestione del rischio IT**. Pensare di evitare tutte le minacce o le vulnerabilità è impossibile, **bisogna organizzarsi per scoprire il prima possibile** falle o attacchi e, nel caso, reagire in maniera mirata e rapida:

- Vulnerability Management
- Continuous Monitoring
- Policy Compliance
- Questionnaire
- PCI Compliance
- Web Application Scanning
- Web Application Firewall
- ThreatProtect

Principali benefici

- Business Continuity
- Protezione da Frodi
- Data Breach prevention (art. 33-34 GDPR)
- Resilienza (capacità di resistere ad un attacco informatico)
- Disponibilità ed integrità delle informazioni