Windows Flaw Exploited to Deliver PowerShell Backdoor

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/llpGV949jbc/windows-flaw-exploited-deliver-powershell-backdoor

---

Microsoft’s Work with Chinese Military University Raises Eyebrows

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/nspeEarofUY/microsofts-work-chinese-military-university-raises-eyebrows

---

Attacker Offers Advice to Matrix.org After Hacking Its Systems

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/iIXng34Hrh4/attacker-offers-advice-matrixorg-after-hacking-its-systems

UK Government Proposes Digital Harms Legislation to Regulate Online Content

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/TtGq8MTZLAk/uk-government-proposes-digital-harms-legislation-regulate-online-content

---

Industry Reactions to New Triton Attacks on Critical Infrastructure

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/_pihUfcoktM/industry-reactions-new-triton-attacks-critical-infrastructure

---

Bayrob Malware Operators

Convicted in the U.S.

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/K47zbPoEkTo/bayrob-malware-operators-convicted-us

---

Data breach, quasi la metà delle aziende non si è adeguata al GDPR. Ecco perché vittime di attacchi

IBM Security ha annunciato i risultati di uno studio globale che esplora la preparazione delle aziende in relazione alla loro capacità di resistere e ripristinare l'operatività in seguito a un attacco cyber.

Condotto dal **Ponemon Institute** e sponsorizzato da **IBM Resilient**, *"2019 Cyber Resilient Organization"* è lo studio annuale sulla resilienza informatica, arrivato alla quarta edizione, che evidenzia la capacità di una azienda di mantenere il proprio scopo primario e la propria integrità alla luce di un attacco informatico.

Il sondaggio è stato condotto a livello globale e riporta le opinioni raccolte da più di 3600 professionisti della sicurezza e dell'IT di tutto il mondo, ha evidenziato come il 77% degli intervistati ha affermato di non avere un piano di risposta agli incidenti di cybersecurity applicato in maniera consistente in tutta l'azienda.

Investire nella sicurezza porta ricchezza

Mentre gli studi mostrano che le compagnie in grado di rispondere in modo rapido ed efficace, contenendo un cyber attacco in 30 giorni, risparmiano in media **oltre 1 milione di dollari** sul costo totale di un data breach, la mancanza di piani di risposta a incidenti di cybersecurity è rimasta costante nell'arco dei quattro anni su cui si è protratto lo studio.

Delle aziende che hanno invece un piano in essere, più della metà (54%) non li testa regolarmente, trovandosi meno preparate a gestire efficacemente i complessi processi e la coordinazione necessari qualora vi sia un attacco.

"*Non pianificare è un piano per fallire rispetto alla necessità di rispondere a un incidente di cybersecurity. I piani di risposta agli incidenti devono essere testati regolarmente e necessitano il pieno supporto del board per investire nelle persone, nei processi e nelle tecnologie necessarie al mantenimento di tale programma,*" afferma **Ted Julian**, VP del Product Management e Co-Founder di IBM Resilient. "*Quando una pianificazione adeguata è affiancata da investimenti nell'automazione, vediamo aziende in grado di risparmiare milioni di dollari durante unattacco*".

L'importanza del GDPR

La prolungata difficoltà che i team di cybersecurity stanno affrontando nell'implementazione di piani di risposta a incidenti di cybersecurity ha impattato la conformità delle imprese alla **General Data Protection Regulation (GDPR**). Quasi metà degli intervistati (46%) afferma che la propria azienda

deve ancora arrivare a una totale ottemperanza del GDPR, persino a un anno dall'anniversario dell'entrata in vigore della legge.

La privacy sempre più prioritaria

Le aziende stanno finalmente riconoscendo che la collaborazione tra privacy e sicurezza informatica migliora la resilienza digitale, con il 62%, che ritengono essenziale l'allineamento dei rispettivi team. La maggior parte degli intervistati crede che il ruolo della privacy stia diventato sempre più importante, specialmente con l'emergere di nuove leggi come il GDPR o il California Consumer Privacy Act, e stanno dando priorità alla protezione dei dati nelle decisioni d'acquisto per l'IT.

Quando richiesto quale fosse il maggior fattore nella giustificazione delle spese per la sicurezza informatica, il 56% delle risposte si concentrava su perdita o furto di informazioni.

Questo risulta particolarmente vero, con i consumatori che richiedono alle aziende di essere maggiormente proattive nella protezione dei propri dati. Secondo una recente ricerca di IBM, il 78% degli intervistati dice che l'abilità di una organizzazione nel proteggere i dati è estremamente importante, con solo il 20% che ha piena fiducia nelle aziende con cui interagisce riguardo il mantenimento della privacy dei propri dati.

In aggiunta, la maggior parte dei partecipanti ha riportato la presenza di un privacy leader in azienda, con il 73% che dice di avere un **Chief Privacy Officer,** provando ulteriormente come la privacy sia diventata una importante priorità per le aziende.

L’automazione è un’area emergente

Per la prima volta, lo studio di quest’anno ha misurato l’impatto dell’automazione sulla resilienza informatica. Nel contesto della ricerca, con automazione si intendono quelle tecnologie di sicurezza che permettono di aumentare o sostituire l’intervento umano nell’identificazione e contenimento di cyber exploit o breach. Queste tecnologie si basano su intelligenza artificiale, machine learning, analytics e orchestrazione.

Quando è stato chiesto se le proprie aziende facessero uso dell’automazione, solo il 23% ha risposto indicando un uso significativo, mentre il 77% ha detto che ne fa un uso moderato, insignificante o nessuno. Le aziende con uso estensivo dell’automazione stimano la propria abilità a prevenire (69% vs 53%), rilevare (76% vs 53%), rispondere (68% vs 53%) e contenere (74% vs 49%) più alta del campione totale di rispondenti.

Lo scarso utilizzo di sistemi automatizzati è un’opportunità mancata per rinforzare la resilienza informatica: infatti, secondo lo Studio sul costo di un Data Breach del 2018, le aziende che implementano l’automazione nei meccanismi di sicurezza risparmiano 1,55 milioni di dollari sul costo totale di un data breach, contrariamente a quanto accade a quelle che non ne fanno uso e che totalizzano un costo molto maggiore per lo stesso tipo di evento.

Lo skills gap impatta ancora la resilienza informatica

Lo skill gap nella cybersecurity sta ulteriormente indebolendo la resilienza informatica, con aziende a corto di personale e impossibilitate a gestire appropriatamente risorse e necessità. I partecipanti al sondaggio hanno riferito che non

dispongono del numero di persone necessarie al corretto mantenimento e test dei propri piani di risposta agli incidenti e che stanno fronteggiando tra le 10 e 20 posizioni scoperte nei propri team di sicurezza. Solo il 30% dei partecipanti ha riportato che il personale per la sicurezza informatica è sufficiente per ottenere un alto livello di resilienza informatica. Inoltre, il 75% degli intervistati ha valutato la propria difficoltà nelle assunzioni e nel mantenimento del personale competente per la sicurezza informatica tra moderatamente alta a alta.

In aggiunta al gap di competenze, quasi la metà dei partecipanti (48%) ha ammesso che le proprie aziende ricorrono a troppi strumenti e soluzioni per la sicurezza, causando una maggiore complessità e riducendo la visione d'insieme sui sistemi di sicurezza.

Per scaricare lo Studio "The 2019 Study on the Cyber Resilient Organization" clicca qui.

https://www.key4biz.it/data-breach-quasi-la-meta-delle-aziende-non-si-e-adeguata-al-gdpr-ecco-perche-vittime-di-attacchi/254066/

WikiLeaks Set 21st Century Model for Cyber-Leak Journalism

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/MZd11uyWjXs/wikileaks-set-21st-century-model-cyber-leak-journalism

Julian Assange: A Decade of Stunning Leaks of U.S. Secrets

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/XEvgEPt-yZg/julian-assange-decade-stunning-leaks-us-secrets

---

Hamas-Linked Threat Actor’s Infrastructure Disrupted

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/4WRUQd9xWMY/hamas-linked-threat-actors-infrastructure-disrupted