



COVER STORY

Un approccio olistico e "analytics driven" alla sicurezza IT con MicroFocus

pag. 4-13

IN QUESTO NUMERO:

CYBER ATTACK

pag. 14-16

Il cybercrime condiziona le nostre vite stando al rapporto Clusit

pag. 17

La Sicurezza IT comincia dal controllo del Multicloud

pag. 18-19

Partecipa all'indagine nazionale sugli attacchi digitali intenzionali in Italia (OAD)

SOLUZIONI

pag. 20-22

Arrow University 2019: cloud, IoT e un business da ripensare

pag. 24-25

Visibilità, velocità e collaborazione contro gli attacchi IT

pag. 26

FortiCWP migliora la security nel cloud e nel multicloud

pag. 28

CyberArk abilita la gestione SaaS degli accessi privilegiati

pag. 30

Consys.it da 25 anni fornisce tranquillità alle imprese

OAD: Osservatorio Attacchi Digitali in Italia

L'OAD, Osservatorio Attacchi Digitali, è l'unica iniziativa in Italia per l'analisi sugli attacchi intenzionali ai sistemi informatici delle aziende e degli enti pubblici in Italia, basata sui dati raccolti attraverso un questionario compilabile anonimamente on line.

Obiettivo principale di OAD è fornire reali e concrete indicazioni sugli attacchi ai sistemi informatici che possano essere di riferimento nazionale, autorevole e indipendente, per la sicurezza ICT in Italia e per l'analisi dei rischi ICT. La disponibilità di un'indagine sugli attacchi digitali indipendente, autorevole e sistematicamente aggiornata (su base annuale) costituisce una indispensabile base per contestualizzare l'analisi dei rischi digitali, richiesta ora da numerose certificazioni e normative, ultima delle quali il nuovo regolamento europeo sulla privacy, GDPR.

La pubblicazione dei rapporti OAD aiutano in maniera concreta all'azione di sensibilizzazione sulla sicurezza digitale del personale a tutti i livelli, dai decisori di vertice agli utenti.

OAD è la continuazione del precedente OAI, Osservatorio Attacchi Informatici in Italia, che ha iniziato le indagini sugli attacchi digitali dal 2008. In occasione del decennale OAD, in termini di anni considerati nelle indagini sono state introdotte numerose innovazioni per l'iniziativa, che includono:

- sito ad hoc come punto di riferimento per OAD e come repository, anno per anno, di tutta la documentazione pubblicata sull'iniziativa OAD-OAI: <https://www.oadweb.it>
- visibilità di OAD nei principali social network: pagina facebook @OADweb, in LinkedIn il Gruppo OAD <https://www.linkedin.com/groups/3862308>
- realizzazione di webinar gratuiti sugli attacchi agli applicativi: il primo, sugli attacchi agli applicativi, è in <https://aipsi.thinkific.com/courses/attacchi-applicativi-italia>
- questionario OAD 2018 con chiara separazione tra che cosa si attacca rispetto alle tecniche di attacco, con nuove domande su attacchi a IoT, a sistemi di automazione industriale e a sistemi basati sulla block chain
- omaggio del numero di gennaio 2018 della rivista ISSA Journal e di un libro di Reportec sulla sicurezza digitale ai rispondenti al questionario OAD 2018
- ampliamento del bacino dei potenziali rispondenti al questionario con accordi di patrocinio con Associazioni ed Ordini di categoria, quali ad esempio il Consiglio Nazionale Forense con i vari Ordini degli Avvocati territoriali
- Reportec come nuovo Publisher e Media Partner
- collaborazione con Polizia Postale ed AgID.

Security & Business n.49
ottobre 2019

Direttore responsabile:
Gaetano Di Blasio

In redazione:
Giuseppe Saccardi, Paola
Saccardi, Edmondo Espa

Hanno collaborato:
Riccardo Florio

Grafica: Aimone Bolliger

Immagini: dreamstime.com

www.securityebusiness.it

Editore:

Reportec srl
Via Marco Aurelio 8
20127 Milano
tel. 02.36580441
www.reportec.it

Registrazione al tribunale
n.585 del 5/11/2010

Tutti i marchi sono
registrati e di proprietà
delle relative società

Nuova cover story su Security & Business, dedicata a Micro Focus e alle sue soluzioni per la protezione delle applicazioni e dei dati, incentrate su un approccio olistico, con un'avanzata tecnologia per l'identity e acces management. All'interno un'intervista esclusiva con Pierpaolo Alì, Director Southern Europe di Micro Focus Security.

Sottolineiamo, in particolare a pagina 18, l'iniziativa AOD (Osservatorio degli Attacchi Digitali), che raccoglie in forma anonima i dati degli incidenti alla sicurezza informatica in Italia. Partecipa anche tu e riceverai un libro omaggio di Reportec e un numero dell'ISSA Journal dedicato agli attacchi dei droni.

La sezione Cyber attack si apre con l'aggiornamento del rapporto Clusit, che, come ogni ottobre, fa il punto sugli attacchi gravi a livello globale, mettendo in allarme non solo il mondo informatico, ma tutti i singoli individui. La trasformazione digitale, infatti, raggiunge tutti e i tanti attacchi che sono stati indirizzati contro strutture ospedaliere dimostrano che il rischio arriva a toccare le persone direttamente sulla loro salute.

Altrettanto importante è la crescita del Cyber Espionage che genera una "Guerra delle informazioni", condizionando l'opinione pubblica e interferendo con la politica e l'economia.

Da sottolineare anche la crescita degli attacchi diretti e l'utilizzo del phishing e del del social engineering.

Nonostante si faccia molta security awareness, il malware e i comportamenti errati da parte degli utenti, restano un pericolo per la protezione nel nuovo mondo digitale.

Il numero contiene anche un mini reportage dell'evento Arrow University, altro importante appuntamento per la sicurezza nel mese a essa dedicato.

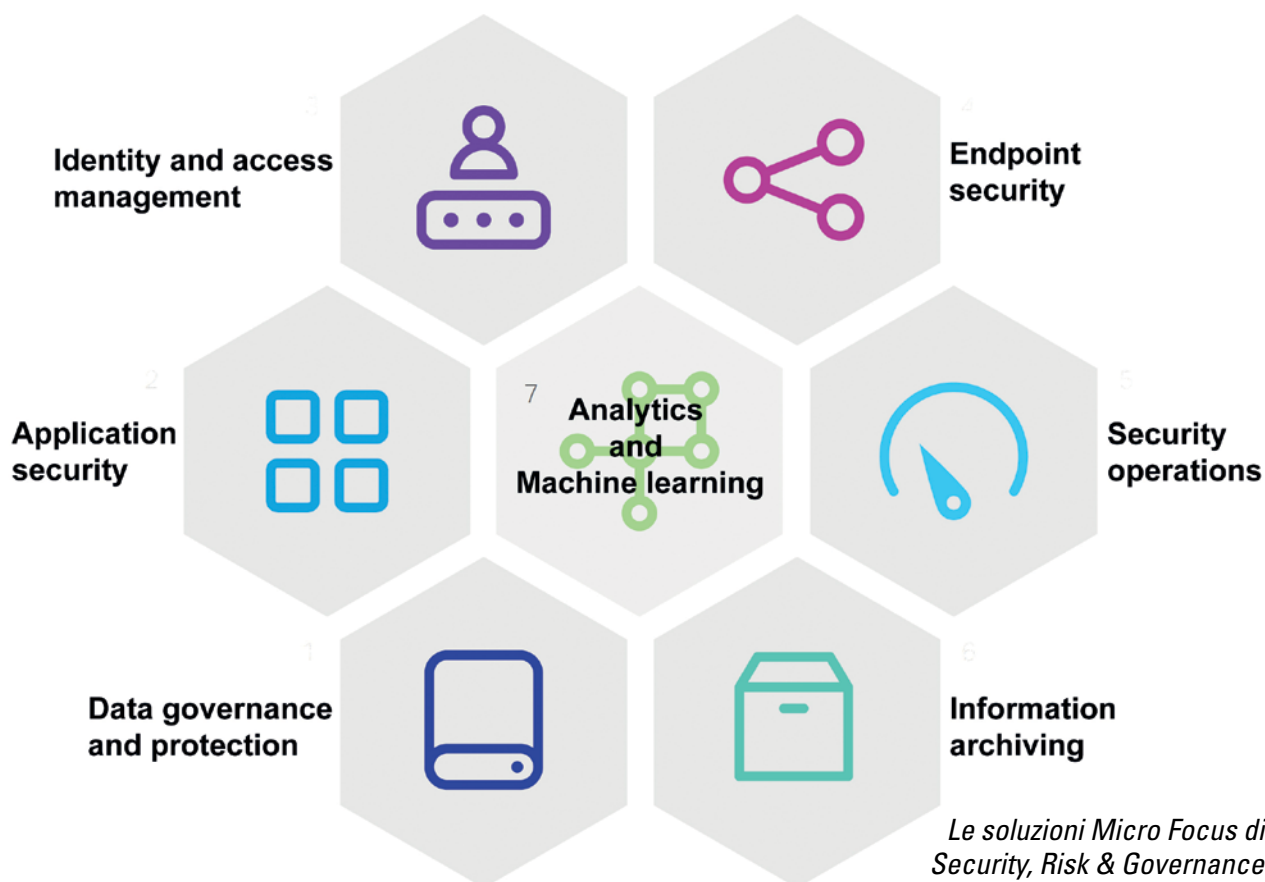
Infine alcune delle ultime soluzioni presentate sul mercato dalle aziende del settore, come Trend Micro, Fortinet, CyberArk e altre.

Prestate attenzioni alle email, a breve riceverete importanti novità sulle nostre testate e sulla prossima campagna abbonamenti.

UN APPROCCIO OLISTICO E "ANALYTICS DRIVEN" ALLA SICUREZZA IT

A differenza di chi propone prodotti di sicurezza puntuali per esigenze specifiche, Micro Focus con le sue soluzioni per il Security, Risk & Governance promuove un approccio olistico e basato su analytics per proteggere identità, applicazioni e dati.

di Riccardo Florio



La crescente complessità è uno dei principali problemi che assilla i responsabili della sicurezza IT. Il costante aumento dei dati, del numero di applicazioni e della frequenza di aggiornamento, degli utenti, dei dispositivi, degli attacchi insieme a requisiti sempre più stringenti di conformità, governance e privacy rendono davvero arduo garantire

un livello di protezione efficace, che non penalizzi l'esperienza degli utenti.

In questo scenario sempre più complesso non stupisce, quindi, che le vulnerabilità aumentino a un ritmo 10 volte più veloce rispetto al passato e che i costi per le aziende abbiano raggiunto livelli sconcertanti. Secondo lo studio di CSO online" Top

cybersecurity facts, figures and statistics for 2018" entro il 2021 la spesa per la sicurezza informatica supererà mille miliardi di dollari e i danni causati dal cyber crimine arriveranno a 6mila miliardi all'anno (il doppio rispetto al 2015); basti pensare che i soli danni da ransomware per il 2019 sono stimati in 11,5 miliardi di dollari.

Un approccio olistico

In risposta a questo scenario Micro Focus promuove un approccio olistico alla sicurezza IT che si basa sull'utilizzo di tecnologie di analytics e machine learning, allontanandosi da un modello basato sul rilascio di soluzioni puntuali dedicate a uno specifico problema.

L'assenza di un approccio olistico e integrato, secondo il vendor, rende più difficile rilevare anomalie e violazioni e limita la capacità di predisporre una pianificazione a lungo termine per la sicurezza informatica e la trasformazione digitale.

In base a questo presupposto, l'insieme di soluzioni di sicurezza proposto da Micro Focus interviene per rispondere ai problemi che interessano gli odierni ecosistemi di tipo ibrido, che spaziano dal mainframe, all'IT tradizionale, al cloud pubblico, fornendo gli strumenti per identificare le minacce, mantenere la compliance, predisporre una protezione preventiva, attivare misure di risposta, proteggere l'accesso, e ripristinare situazioni compromesse.

«Micro Focus - spiega Pierpaolo Ali, Director

Southern Europe di Micro Focus Security - è il partner ideale per aiutare le aziende a perseguire un approccio olistico alla sicurezza. Siamo tra i pochissimi fornitori in grado di fornire soluzioni per la difesa da violazioni, per rendere sicuro il processo di sviluppo del software, tutelare la privacy delle persone, gestire l'accesso e l'identità, rendere sicure le applicazioni, proteggere i dati e aiutare le aziende a conformarsi alle normative».

Una famiglia di soluzioni per ogni esigenza di sicurezza

Il modello di Security, risk and governance proposto da Micro Focus punta a supportare le aziende nella protezione delle tre dimensioni di rischio: identità, dati e applicazioni. A ognuna di queste esigenze è dedicata una famiglia specifica di soluzioni software. La famiglia di soluzioni e tecnologie di security intelligence ArcSight è la soluzione SIEM (Security Information and Event Management) integrata per la raccolta di dati di sicurezza, la loro analisi e la

Entro il 2021 la spesa per la sicurezza informatica supererà mille miliardi di dollari e i danni causati dal cyber crimine arriveranno a 6mila miliardi all'anno

predisposizione di misure preventive contro possibili minacce.

Le soluzioni Micro Focus NetIQ si occupano dei rischi associati alla componente umana, affrontando le tematiche di gestione delle identità digitali e di predisposizione di modelli di accesso flessibili e sicuri.

Al tema della protezione dei dati sono dedicate le soluzioni Voltage SecureData Enterprise, che prevedono innovative tecnologie di cifratura dei dati nel corso del loro intero ciclo di vita.

Fortify è l'insieme di soluzioni per la sicurezza applicativa a partire dalla fase di sviluppo, adatte per applicazioni interne, commerciali e disponibili anche per effettuare test on-demand.

Le soluzioni Micro Focus per la Governance (Secure

Content Management suite, Collaboration suite, Digital Safe e Retain) permettono, infine, di gestire in modo sicuro le informazioni durante tutto il loro ciclo di vita, in base a una politica di governance continua che si estende dalla classificazione dei dati alla gestione e trattamento a lungo termine.

«Micro Focus - conclude Alì - ritiene che le aziende non debbano eliminare il passato per aprirsi al futuro. Tutto ciò che facciamo è basato sull'idea che il modo più rapido e sicuro per ottenere risultati sia quello di costruire su ciò che si ha. Le nostre soluzioni fanno proprio questo: colmano il divario tra le tecnologie esistenti ed emergenti così da poter accelerare il processo di innovazione verso la trasformazione digitale, con meno rischi». ❁

UNA SICUREZZA OLISTICA E INTELLIGENTE PER DATI, IDENTITÀ E APPLICAZIONI

Pierpaolo Alì, Director Southern Europe di Micro Focus Security, delinea lo scenario evolutivo delle esigenze di sicurezza e fornisce indicazioni per proteggere, in modo efficace, ciò che conta di più per un'azienda. *di Riccardo Florio*

Security & Business: La sicurezza aziendale va ripensata?

Pierpaolo Alì: «Stiamo assistendo negli ultimi anni ad una grande accelerazione, ciò che fino a qualche tempo fa era richiesto in qualche giorno oggi deve essere fornito in poche ore, questo impatta il ns modo di vivere, lavorare e naturalmente il modo di fare sicurezza. Oggi il principale creatore

Pierpaolo Ali, Director Southern Europe di Micro Focus Security



di contenuti (Google N.d.R.) non ha un giornalista, la principale catena alberghiera (Airbnb N.d.R.) non possiede alcun Hotel e la prima azienda di trasporto automobilistico privato (Über N.d.R.) non è proprietaria di neppure un'autovettura. Questo esempio mette in evidenza come i modelli di business siano completamente cambiati nel tempo e con essi sono mutati il valore degli asset digitali, le tipologie di rischio e le modalità di protezione.

S&B: «Come deve essere quindi la sicurezza del nuovo millennio?»

P.A.: «Deve essere, innanzitutto, una sicurezza non più incentrata sulla difesa del perimetro aziendale che, di fatto, non esiste più. La protezione deve essere multidimensionale e intervenire per esercitare un'adeguata governance delle tre dimensioni di rischio: dati, utenti e applicazioni.

Per essere davvero efficace, la protezione deve essere esercitata durante l'intero ciclo di vita dei dati, delle applicazioni e delle identità digitali, ponendo massima attenzione ad aspetti, talvolta trascurati, quali la fase di sviluppo delle applicazioni, la rimozione di un'identità digitale aziendale o la cancellazione sicura dei dati.

S&B: « Possiamo dare delle indicazioni concrete in relazione a ognuno dei tre aspetti che ha citato, cominciando dai dati?»

P.A.: « Rendere sicuro il dato significa predisporre

le condizioni per esercitare la protezione in ogni istante, non solo in alcune fasi. Molte soluzioni di sicurezza si concentrano sulla protezione del dato quando è a riposo ovvero archiviato oppure mentre viene spostato attraverso

la rete, evitando di proteggerlo mentre è in esercizio. Questo perché si tratta di un compito molto difficile che Micro Focus riesce a realizzare grazie a un brevetto esclusivo. La tecnologia Micro Focus permette di mantenere il dato cifrato mentre viene utilizzato: neppure l'operatore, se non autorizzato, ha la possibilità di vedere il dato in chiaro. Se il dato venisse sottratto non avrebbe alcun valore.

S&B: Per quanto riguarda le applicazioni?»

P.A.: «Le applicazioni sono, attualmente, il principale veicolo di vulnerabilità all'interno di qualsiasi rete aziendale. Il modello di sviluppo applicativo punta, spesso, più alla rapidità di rilascio che alla cura della sicurezza.

Micro Focus, con la gamma Fortify, mette a disposizione una serie di soluzioni che intervengono durante la fase di sviluppo, per testare in tempo reale, mentre il codice viene scritto, se vi sono vulnerabilità e suggerendo modifiche al codice per evitarle. Una volta terminata la parte di sviluppo sicuro, grazie agli strumenti di test di Micro Focus è possibile verificare la presenza delle vulnerabilità applicative a riposo o in produzione. Tutto ciò anche in modalità on-demand e anche su applicazioni commerciali.

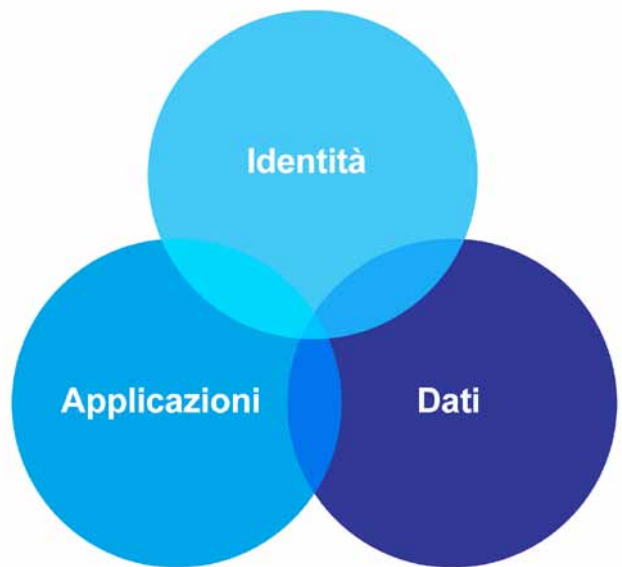
S&B: « *Gli utenti solitamente sono considerati l'anello più debole della catena di sicurezza. Qual è la vostra ricetta di sicurezza?* »

P.A.: «I comportamenti degli utenti sono certamente quelli che mettono più a rischio l'azienda e l'invito a una cultura della sicurezza pervasiva va sempre rimarcato. Tuttavia, spesso le aziende non mettono in atto le misure di protezione disponibili e che possono limitare al minimo questo rischio.

Attraverso la famiglia di soluzioni NetIQ Micro Focus consente una gestione delle identità e dell'accesso che riduce al minimo il rischio di possibili violazioni avvalendosi di tecniche avanzate di "intelligent security".

S&B: « *E per rispondere agli attacchi da Internet e alle nuove minacce?* »

P.A.: «Lo sviluppo in termini numerici e qualitativi dei nuovi attacchi è giunto a un tale livello che non è più possibile delegare la difesa unicamente all'intervento e alla capacità umana. Continuare a raccogliere enormi volumi di log di sicurezza senza predisporre le condizioni per analizzarli e interpretarli efficacemente è una perdita di tempo e di denaro. Per questo motivo Micro Focus ha sviluppato la famiglia di soluzioni di security intelligence ArcSight, che Gartner da 13 anni di seguito inserisce tra i leader all'interno del Magic Quadrant per le soluzioni di Security Information and Event Management. Queste soluzioni sono sorrette dalle più avanzate tecnologie di analytics e intelligenza artificiale.



Vorrei ricordare, per esempio, la nota piattaforma di analytics Vertica e la soluzione Intersect, recentemente entrata nel nostro portfolio con l'acquisizione dell'omonima società, che fornisce algoritmi di intelligenza artificiale e machine learning per l'analisi comportamentale.

S&B: « *Con quale approccio un'azienda dovrebbe affrontare le nuove sfide di sicurezza?* »

P.A.: «È fondamentale considerare la sicurezza come un processo pervasivo e intrinseco e non come una sovrapposizione a posteriori di tecnologie e applicazioni sull'infrastruttura aziendale. Questo processo va inserito in un modello di governance e gestione del rischio partendo da un assessment degli asset aziendali.

Le soluzioni Micro Focus di Security, Risk & Governance mettono a disposizione un ecosistema di analisi che permette di classificare i dati aziendali più a rischio all'interno di migliaia di tipi di contenuto, di applicare policy in oltre 160 ambiti e di proteggere le informazioni critiche. ❁



DATI SEMPRE CIFRATI DURANTE IL CICLO DI VITA

Le soluzioni Voltage Secure Data si avvalgono di esclusive tecnologie brevettate per assicurare che i dati sensibili restino sempre cifrati, anche quando vengono utilizzati dalle applicazioni

di Riccardo Florio

Assicurare la protezione dei dati è un'esigenza crescente, sia per l'importanza sempre maggiore che i dati rivestono per il business aziendale, sia per i nuovi modelli di business pensati per favorire la condivisione delle informazioni.

Nel corso degli anni sono state sviluppate diverse tecnologie di cifratura e mascheramento che vengono però, tipicamente, applicate occasionalmente in specifiche situazioni: per esempio prima di effettuare un trasferimento via rete.

L'importanza dei dati richiede, invece, una protezione esercitata in ogni istante del loro ciclo di vita. Attraverso le soluzioni Voltage SecureData Enterprise Micro Focus risponde a questa esigenza proponendo un approccio dato-centrico in cui il dato viene cifrato al momento della sua creazione e resta sempre oscurato, portando con sé le policy di sicurezza che lo riguardano.

La tecnologia Hyper FPE

Questo risultato è ottenuto grazie a tecnologie esclusive brevettate come Hyper Format-Preserving

Encryption (FPE), uno standard di cifratura riconosciuto dal NIST, che consente di cifrare i dati preservandone il formato originale ovvero la loro integrità referenziale, che ne garantisce l'usabilità per le operazioni di elaborazione, le applicazioni e i servizi. Per esempio, l'insieme di campi che identifica un utente e le sue coordinate bancarie viene alterato da Hyper FPE ma mantiene lo stesso formato così da poter essere trattato all'interno di un database e utilizzato per effettuare verifiche, analisi e associazioni in modo consistente attraverso tabelle e data set. Questo è un requisito importante quando si devono gestire insiemi di dati inseriti in Hadoop e ancor più critico quando vengono utilizzati identificatori comuni come il codice fiscale o la carta di identità come riferimenti comuni tra insiemi di dati diversi. In questo modo i dati critici restano sempre cifrati e, anche in caso di furto e/o diffusione non autorizzata, risultano completamente inutilizzabili, sollevando anche l'azienda dall'obbligo normativo di segnalare all'autorità competente l'avvenuta sottrazione.



SICUREZZA DELLE APPLICAZIONI PER RIDURRE LE VULNERABILITÀ

di Riccardo Florio

Le applicazioni sono la principale fonte di vulnerabilità e richiedono una protezione che si estenda al loro intero ciclo di vita. A questa esigenza si indirizza la famiglia di soluzioni Micro Focus Fortify. La capacità di gestire il patrimonio applicativo è diventata un fattore di differenziazione competitiva per molte aziende che si trovano, sempre più spesso, a dover faticare per proteggere le proprie applicazioni a causa della mancanza di integrazione della sicurezza nei processi di sviluppo e nella fase operativa.

A rendere ancora più complesso il compito contribuiscono la carente disponibilità di competenze nella sicurezza delle applicazioni e la difficoltà a tenere il passo con l'elevata frequenza dei loro aggiornamenti. Le applicazioni rappresentano oggi la principale fonte di vulnerabilità e il punto di ingresso privilegiato dai cyber criminali per le attività illecite anche perché le soluzioni di sicurezza network-based sono inefficaci contro questo tipo di minaccia.

Troppe applicazioni sono distribuite con bassi livelli di sicurezza delegando al rilascio successivo delle patch il compito di aggiustare le cose. Tra le carenze più frequenti si possono citare: un'autenticazione debole, cattive pratiche di sviluppo e una cattiva gestione dei dati.

L'affermazione delle pratiche DevOps accelera il rilascio delle applicazioni ma, senza predisporre una buona sicurezza integrata, DevOps accelererà anche la diffusione delle vulnerabilità. Per questo motivo è essenziale che le pratiche di sicurezza siano previste dall'inizio aumentando la capacità delle applicazioni di resistere alle minacce interne ed esterne.

Protezione durante il ciclo di vita con Fortify

La gamma Fortify aggruppa una serie di strumenti pensati per favorire uno sviluppo sicuro che elimini alla fonte le possibili vulnerabilità. Le soluzioni Micro Focus si avvalgono anche di tecnologie RASP (Runtime Application Self Protection) che integrano all'interno delle applicazioni la capacità di analizzare il codice all'interno dell'ambiente di produzione per attuare contromisure in modo autonomo e automatizzato: per esempio bloccare l'accesso verso Internet in caso di situazioni sospette.

GOVERNANCE DELL'IDENTITÀ SICURA CON NETIQ

Le identità si sono evolute e non sono più univocamente associate agli individui, ma comprendono anche dispositivi, cose e servizi tipicamente esterni all'azienda e distribuiti geograficamente. Per questa



Attraverso Fortify Static Code Analyzer è possibile predisporre ambienti di test di tipo statico per rendere sicuro il codice durante la fase di sviluppo. Questa



soluzione, grazie all'integrazione con strumenti come Visual Studio, JIRA, ALM Octane e Jenkins, permette di predisporre meccanismi automatizzati di controllo durante la fase di sviluppo, favorendo la creazione di codice sorgente privo di vulnerabilità.

Fortify WebInspect è invece lo strumento per effettuare test dinamici sulla sicurezza delle applicazioni Web e test di penetrazione in modo dinamico e in tempo reale, anche sulle applicazioni commerciali. Attraverso la soluzione Fortify on Demand Micro Focus permette di effettuare i test di tipo statico e dinamico anche in modalità di servizio on-demand senza richiedere l'acquisto di hardware né l'installazione di alcun software



Il modello di gestione dell'identità dalle soluzioni Micro Focus NetIQ si raccorda con gli strumenti di sicurezza unificando in modo coerente i temi di Identity governance, accesso sicuro e monitoraggio dell'attività degli utenti

di Riccardo Florio

ragione gestire l'identità significa monitorare non solo chi, ma anche cosa richiede l'accesso a dati e sistemi e se il livello di accesso richiesto è coerente con i privilegi. Inoltre, un insieme sempre più ampio di tipologie di aziende si trova a dover gestire anche le identità esterne come quelle dei clienti, al fine di migliorare la loro esperienza mantenendo il rispetto della privacy. Attraverso il set di soluzioni NetIQ Micro Focus fornisce una risposta a tutte queste esigenze con strumenti pensati per proteggere efficacemente l'identità digitale fatta di credenziali, attributi e ruoli, nonché di governare le modalità di accesso e i privilegi associati.

La governance delle identità

Le soluzioni NetIQ di Micro Focus consentono di realizzare una Identity governance centralizzata di tipo adattativo per assicurare la conformità normativa, migliorare l'esperienza dell'utente, ridurre il rischio minimizzando la superficie di attacco e gestire l'accesso in modo più efficace.

L'automazione dei processi di identità, provisioning e approvazione abilitata dalle soluzioni NetIQ consente alle aziende di rendere accessibili le risorse aziendali necessarie ai propri dipendenti già dal primo giorno di lavoro. L'accesso è reso sicuro grazie a strumenti di autenticazione multifattore oltre all'uso

di funzioni di Single Sign-On che si estendono attraverso ambienti cloud, mobile e la rete enterprise. Grazie a questi strumenti le identità vengono mantenute coerenti e sincronizzate evitando i possibili problemi che derivano dal possesso di più identità sovrapposte all'interno dell'azienda (per esempio associate a progetti speciali o a molteplici ruoli o funzioni) e predisponendo la cancellazione immediata e automatica dei privilegi quando un utente non è più in azienda. Attraverso questa governance degli accessi si concretizza il principio del minimo privilegio in base al quale un utente deve disporre di tutti e soli i privilegi necessari per lo svolgimento del suo lavoro. Per monitorare l'attività degli utenti le soluzioni Micro Focus si avvalgono di tecnologie di security intelligence che accelerano sia l'identificazione delle minacce sia l'attivazione di azioni di risposta. Tra le funzionalità specifiche disponibili nella famiglia NetIQ merita di essere ricordata quella per la gestione degli account privilegiati la cui eventuale compromissione, per la tipologia di informazioni a cui hanno accesso, è in grado di avere ripercussioni critiche per l'azienda.

Il modello proposto da Micro Focus attraverso le soluzioni NetIQ riunisce, dunque, il tema della gestione della sicurezza con la gestione delle identità e degli accessi (spesso scorrelati in azienda) evidenziando l'obiettivo comune di protezione delle informazioni. Questo significa integrare le informazioni associate all'identità all'interno degli strumenti di monitoraggio della sicurezza, fornendo l'indispensabile "contesto di identità" di cui i team hanno bisogno per riconoscere e affrontare i potenziali attacchi nel modo più rapido possibile. ❁

PREVENIRE LE MINACCE CON ARCSIGHT

Micro Focus ArcSight è la piattaforma SIEM che sfrutta tecnologie di analytics e machine learning per l'analisi in tempo reale e la correlazione di tutti i log di sicurezza

di Riccardo Florio

L'impossibilità di gestire il crescente scenario di minacce sta portando all'implementazione di tecnologie di analytics e alla diffusione di soluzioni per il monitoraggio delle informazioni e degli eventi di sicurezza, solitamente indicate con l'acronimo SIEM (Security Information and Event Management).

Attraverso le soluzioni ArcSight, Micro Focus propone una gamma di soluzioni e tecnologie di security intelligence in grado di monitorare con continuità l'intera infrastruttura aziendale correlando in tempo reale log, ruoli dell'utente e flussi di rete per individuare possibili minacce, incluse quelle di nuovo tipo.

La piattaforma ArcSight ha un'impostazione modulare e può essere facilmente inserita all'interno dell'infrastruttura aziendale esistente interagendo con soluzioni di sicurezza multivendor.

Le tecnologie Vertica e Interset forniscono gli strumenti di analytics e controllo delle anomalie che

alimentano il motore di correlazione e individuazione delle possibili minacce.

I principali componenti della famiglia ArcSight

I tasselli fondamentali della soluzione sono ArcSight ADP e ArcSight ESM.

ArcSight Data Platform (ADP) mette a disposizione oltre 400 connettori pronti all'uso e un tool per la creazione di connettori personalizzati, permettendo di raccogliere dati praticamente da ogni tipo di fonte esistente: log, sensori, flussi di rete, apparati di sicurezza, Web server, applicazioni custom, social media, servizi cloud e altre.

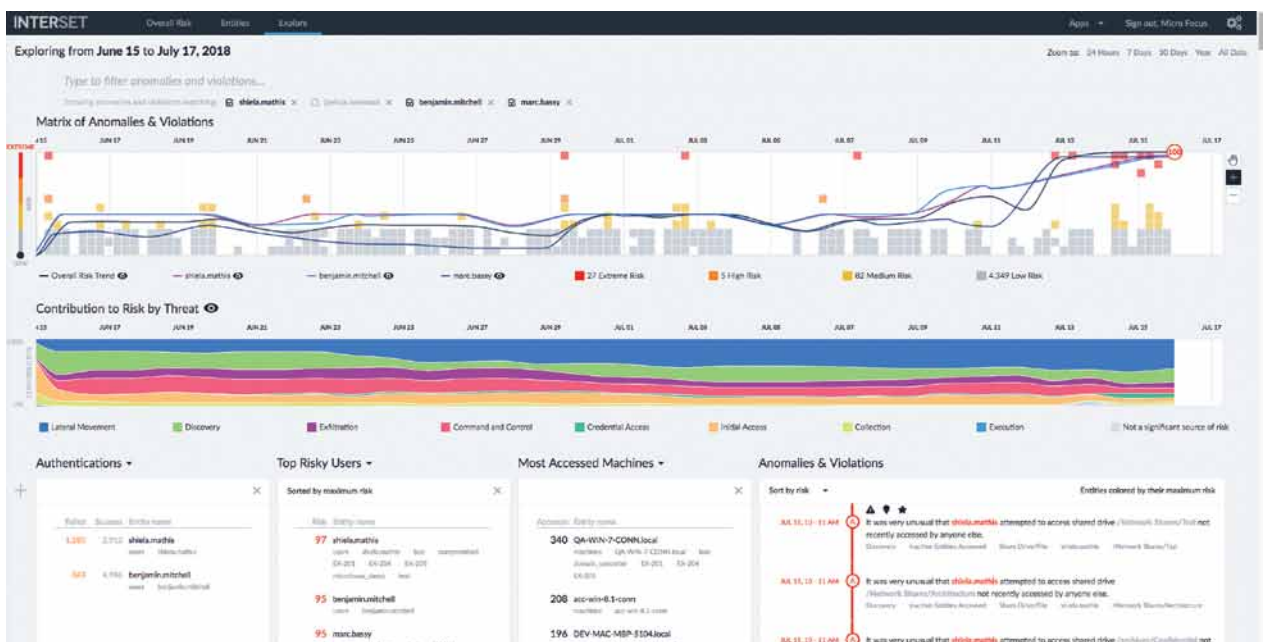
ArcSight Enterprise Security Manager (ESM) è la soluzione per la raccolta, l'analisi e la correlazione delle informazioni di sicurezza capace di identificare possibili minacce stabilendo la tipologia e la priorità di interventi per fronteggiare efficacemente.

Le capacità di rilevamento delle minacce fornita dalle soluzioni di predictive security della famiglia

ArcSight possono essere ulteriormente ampliate e accelerate tramite ArcSight Investigate.

Intersect: un nuovo modo di analizzare i comportamenti

Intersect è l'ultimo arrivo in casa Micro Focus Security (a seguito dell'acquisizione dell'omonima azienda a febbraio 2019), attualmente in fase di integrazione all'interno della famiglia di soluzioni ArcSight. È una tecnologia per l'analisi dei comportamenti degli utenti che utilizza algoritmi di auto apprendimento per individuare eventi anomali e capace di rimodellare in modo autonomo e costante le proprie modalità di analisi e i criteri di definizione degli indici di rischio. Il risultato è un nuovo tipo di analisi comportamentale, che riesce a identificare situazioni anomale rispetto a un'esperienza dell'utente che muta nel tempo, slegandosi da modelli deterministici e/o basati sul superamento di soglie. ❄



Esempio d'un'analisi delle anomalie

IL CYBERCRIME CONDIZIONA LE NOSTRE VITE STANDO AL RAPPORTO CLUSIT

L'aggiornamento del rapporto con i dati del primo semestre mostra la preoccupante crescita di alcuni attacchi, in particolare diretti contro le strutture della Sanità

di Gaetano Di Blasio

Nel primo semestre del 2019 ben 97 attacchi su 757 (ricordiamo che vengono presi in considerazione dal Clusit solo quelli più gravi a livello globale) sono stati indirizzati in un settore che ha un impatto importante e diretto con la salute dei cittadini: la sanità. In questo settore non si era mai arrivati agli attuali livelli.

Complessivamente, a prescindere dal comparto economico, si tratta di una media mensile di 126, che rappresenta una crescita modesta pari all'1,3%. Una nota positiva, ma che non deve trarre in inganno: infatti, la concentrazione degli attacchi, da parte del cybercrime (cioè gli attacchi che il Clusit considera diretti a ricavare denaro, come il ransomware o lo spionaggio industriale), mette in luce la determinazione verso bersagli mirati, che generalmente provocano danni maggiori e alzano il livello di rischio.

Inoltre, il cybercrime, che pesa per l'85% degli attacchi ed è incrementato dell'8,3% rispetto al numero di attacchi registrati nel primo semestre 2018, si accompagna con la forte crescita dei vettori di attacco basati su Phishing e Social Engineering, che

registrano un più 104%.

Sul fronte del cyber spionaggio gli esperti del Clusit registrano una situazione stabile, così come per la cosiddetta "Information Warfare" (la guerra delle informazioni). Ma occorre considerare che tali attività sono meno evidenti e difficili da stimare con certezza.

I livelli d'impatto

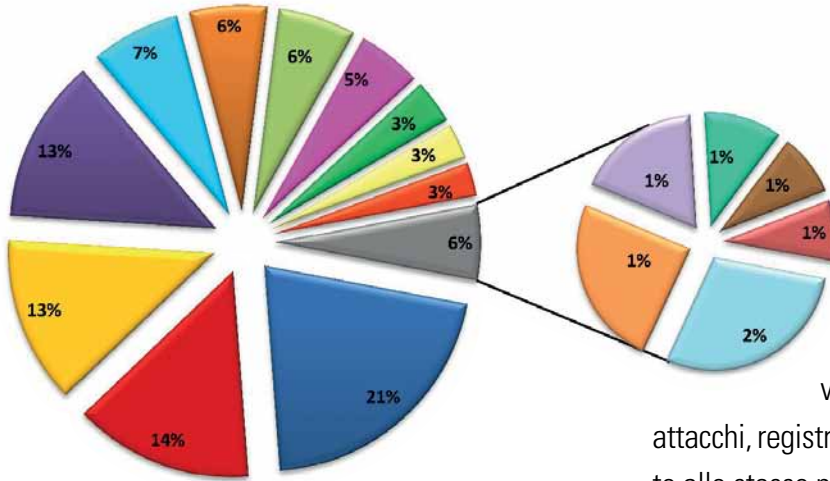
Come da un paio di anni a questa parte, gli autori del rapporto valutano gli attacchi in base ai livelli d'impatto, che rappresenta un dato più accurato rispetto al "semplice" conteggio del numero di attacchi. L'analisi presentata al Security Summit di Verona 2019, rileva che

L'analisi dei "livelli di impatto", condotta per ogni singolo attacco, mostra inoltre che, nonostante il cybercrime sia numericamente dominante, gli effetti dei singoli attacchi sono di gravità inferiore, rispetto ad altre tipologie di minacce alla sicurezza. Andrea Zapparoli Manzoni, membro del Comitato Direttivo Clusit, nonché uno degli autori del rapporto avanza un'ipotesi su questa apparente contraddizione, dovuta all'esigenza, da parte dei criminali informatici, di dover mantenere un profilo relativamente basso per continuare ad agire senza attirare troppa attenzione.

Peraltro, Zapparoli Manzoni evidenzia: « Pur avendo una Severity media più bassa, dati i numeri in gioco gli attacchi con finalità cyber-criminale generano comunque la maggior parte dei danni a livello globale».

Tipologia e distribuzione % delle vittime - 1H 2019

© Clusit - Rapporto 2019 sulla Sicurezza ICT in Italia - Aggiornamento Giugno 2019



territoriali e dalla tipologia dei bersagli, puntando solo a massimizzare il risultato».

Il triste elenco di "attaccati" prosegue con la categoria "Online Services / Cloud", colpita dal 14% degli

attacchi, registrando un incremento del 49,3% rispetto allo stesso periodo dello scorso anno.

Come già evidenziato, la sanità è al centro del mirino, avendo subito, tra gennaio e giugno 2019, una crescita degli attacchi pari al 31% rispetto allo stesso periodo del 2018.

Si tratta, sottolinea nano gli autori del rapporto del maggior "bombardamento" indirizzato su uno specifico settore dal 2011 (anno della pubblicazione del primo Rapporto Clusit).

Sul podio dei settori più cercati dai criminali informatici, sale il retail/GDO (Grande distribuzione organizzata) con un incremento degli attacchi che arriva al 40,0%.

Diminuiscono, invece, gli notevolmente attacchi gravi noti, indirizzati alle categorie: "Government" (-17,5%) e "Banking / Finance" (-35,4%).

Praticamente stabili le altre categorie.

Le tecniche d'attacco

Gli esperti del Clusit hanno analizzati i dati relative alle tecniche di attacco, cui gli addetti ai lavori faranno bene a porre attenzione, per prendere le contromisure necessarie.

In particolare, è emerso che, nel primo semestre 2019, al fine di realizzare i propri intenti criminali,

L'esperto del Clusit aggiunge anche: «Dal 2016 assistiamo anche alla diffusione di attività cyber-criminali spicchiole, quali le quotidiane campagne mirate a compiere truffe ed estorsioni realizzate tramite phishing e ransomware, che hanno colpito anche moltissime organizzazioni e cittadini italiani; confermiamo che questo trend si è rafforzato nel triennio 2017-2019 ed è tuttora in crescita».

I settori più colpiti

Nel primo semestre del 2019, il maggior numero di attacchi si concentra in una categoria mista, indicata dal Clusit come "Multiple Targets", che raccoglie il 21% delle vittime che hanno subito attacchi comuni, in aumento del 16,3% rispetto allo stesso semestre del 2018. Sono attacchi compiuti in parallelo dallo stesso gruppo di attaccanti contro molteplici organizzazioni appartenenti a categorie differenti. Gli esperti ritengono che tali caratteristiche confermano quanto tutti possono essere "bersagli" e, inoltre, dimostra che « gli attaccanti sono diventati sempre più aggressivi ed organizzati e possono condurre operazioni su scala sempre maggiore, con una logica "industriale", a prescindere da vincoli

gli attaccanti si sono potuti affidare a semplici malware, prodotti "industrialmente" a costi bassi e decrescenti, cui si aggiungono tecniche di Phishing e Social Engineering, come su accennato.

Le tecniche sconosciute, classificate dal Clusit come categoria "Unknown" restano al secondo posto, con un aumento registrato del 23,8%, rispetto al primo semestre 2018. Cresce del 5,1% più di tutti il malware che si conferma al primo posto assoluto, rappresentando il 41% del totale nel periodo (contro il 38% nel primo semestre 2018).

Gli autori del rapporto, peraltro, ritengono importante "sommare" la crescita del malware semplice con quello della categoria Multiple Techniques / APT, cioè gli strumenti degli attacchi persistenti e mirati, che spesso sfruttano i malware per orchestrare attacchi più sofisticati.

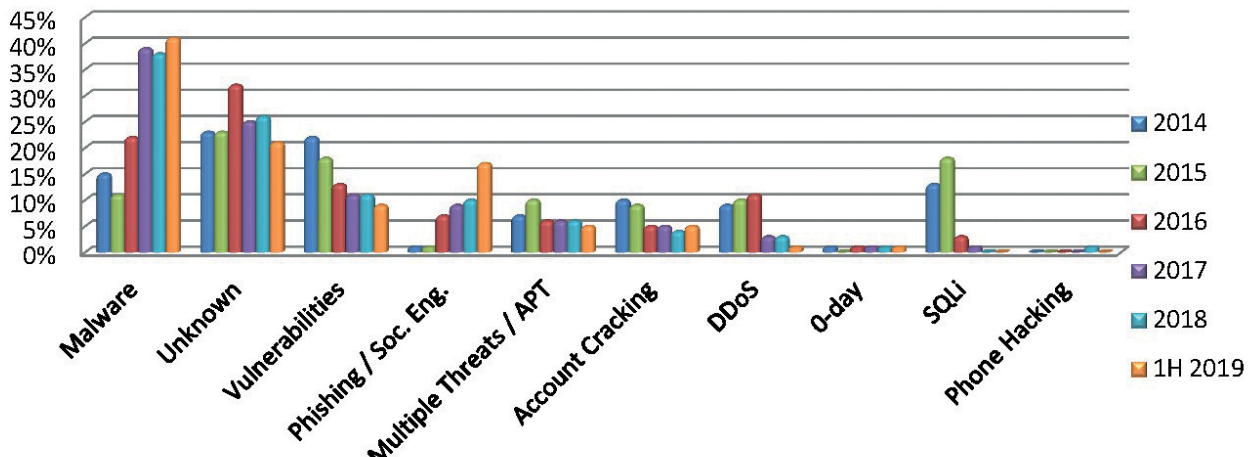
In sostanza, gli esperti ritengono che il malware sia protagonista nel 45,5% delle tecniche di attacco utilizzate.

Un altro dato da considerare riguarda il significativo ritorno alla crescita degli attacchi basati su tecniche di "Account Hacking /Cracking" (+88,9% rispetto al primo semestre 2018).

Sul fronte dei dispositivi mobili, viene segnalato l'utilizzo di malware specifico per piattaforme mobile l'11% del totale (6% Android, 5% iOS) dei malware osservati.

In buona sostanza, i "cattivi" restano in vantaggio, come chiosa Zapparoli Manzoni: «Considerato che stiamo analizzando gli attacchi più gravi del primo semestre 2019, compiuti contro primarie organizzazioni pubbliche e private, spesso di livello mondiale, il fatto che la somma delle tecniche di attacco più banali, quali SQLi, DDoS, Vulnerabilità note, Account cracking, Phishing e Malware "semplice", rappresenti ancora il 63% del totale implica che gli attaccanti possono realizzare attacchi gravi di successo contro le loro vittime con relativa semplicità e a costi molto bassi, oltre tutto decrescenti». ✨

Distribuzione tecniche di attacco - 2014 - 1H 2019



LA SICUREZZA IT COMINCIA DAL CONTROLLO DEL MULTICLOUD

di Giuseppe Saccardi

Più dati transitano da e verso il cloud pubblico, più cresce l'esigenza di proteggere gli scambi tra endpoint e piattaforme

È un dato di fatto che la sempre più pervasiva adozione di servizi cloud da parte delle aziende sta determinando una continua e crescente migrazione di dati verso ambienti remoti e distribuiti e di conseguenza la necessità per i team di sicurezza di alzare il livello di protezione delle informazioni sensibili in contesti multi o hybrid cloud.

Le indagini condotte da IDC evidenziano come molte imprese stiano estendendo il portafoglio di soluzioni di sicurezza IT come parte del meccanismo di attuazione delle policy per l'utilizzo di risorse cloud, andando a integrare in questo portafoglio nuovi software o servizi come i Cloud Access Security Broker.

I dati parlano da soli ed evidenziano l'ampiezza del problema. La spesa mondiale in soluzioni per la sicurezza web crescerà secondo IDC con un tasso composto medio annuo (CAGR) del +9,8% al 2022.

La componente di cloud pubblico (SaaS) di questa spesa farà segnare un CAGR del +14% nello stesso periodo, quella on-premise del +5,1%. A guidare questa crescita saranno soprattutto i Cloud Access Security Broker (CASB, conosciuti anche come Cloud Security Gateway), e i Web Application Firewall. In particolare, i Cloud Access Security Broker stanno diventando un tassello fondamentale del puzzle della sicurezza cloud.



Più spazio per i Cloud Access Security Broker

Considerate le enormi opportunità che possono nascere per le aziende dall'aggregazione di dati di molteplici applicazioni SaaS, queste soluzioni rappresentano il punto di controllo essenziale negli scambi di informazione tra gli end point e le piattaforme cloud, tra le Operation Technologies e i data center di nuova generazione.

Per i Cloud Access Security Broker si sta in sostanza aprendo in questo momento una seconda fase importante. Nella prima, la loro adozione è stata dettata soprattutto dall'esigenza da parte delle aziende di governare e avere visibilità degli accessi al web. In questa seconda fase, l'accento si è spostato, ma è meglio dire esteso, alla protezione dei dati, ovunque essi si trovino allocati. La necessità per le imprese di "vedere" e "proteggere" interponendo un punto di controllo tra utenti e risorse cloud, osserva IDC, spiega l'incessante richiesta per questa tipologia di soluzioni, nonché per modelli contrattuali di condivisione delle responsabilità in cui gli obblighi di sicurezza e conformità siano ripartiti nella maniera più efficace possibile tra il fornitore e il cliente.

PARTECIPA ALL'INDAGINE NAZIONALE SUGLI ATTACCHI DIGITALI INTENZIONALI IN ITALIA (OAD)

È in pieno corso l'iniziativa OAD, Osservatorio Attacchi Digitali in Italia, giunta all'undicesimo anno consecutivo di indagine on line sugli attacchi intenzionali ai sistemi informatici di aziende ed enti, di qualsiasi dimensione (come numero di dipendenti) ed operanti in Italia: dalle aziende manifatturiere a quelle di servizi, dagli studi professionali agli esercizi commerciali ed alberghieri, dalle scuole e università alle ASL e agli ospedali, dai Comuni alle Province, dalle Regioni ai Ministeri.

L'iniziativa OAD

OAD è una iniziativa di MALABO Srl (www.malabo-advisoring.it), la società di consulenza direzionale sull'ICT dell'autore Marco R. A. Bozzetti che realizza l'indagine on line, elabora i dati raccolti e stende il rapporto finale, in collaborazione con AIPSI, Associazione Italiana Professionisti Sicurezza Digitale, capitolo italiano di ISSA (www.aipsi.org, www.issa.org), con l'editore Reportec Srl (www.reportec.it), e con la Polizia Postale e delle Telecomunicazioni (<https://www.commissariatodips.it/>), che fornisce dati essenziali sugli attacchi alle infrastrutture critiche e a quelle finanziarie, incluso il numero di denunce e di arresti. L'OAD, Osservatorio Attacchi Digitali in Italia, è l'unica iniziativa in Italia per l'analisi sugli attacchi intenzionali ai sistemi informativi delle Aziende e degli Enti Pubblici italiani, **realizzata tramite una indagine anonima indirizzata a tutte le aziende e alle Pubbliche Amministrazioni** di ogni settore merceologico e dimensione, **tramite un questionario compilabile on line con un browser**.

Il questionario è rivolto principalmente ai Responsabili dei Sistemi Informativi e della Sicurezza Informatica.

Sulla base delle risposte anonime al questionario, opportunamente elaborate e sintetizzate, viene preparato un Rapporto finale gratuitamente scaricabile dal sito web <https://www.oadweb.it/>, che costituisce l'archivio storico di tutti i rapporti pubblicati, e di tutte le presentazioni ed articoli che su di essi sono stati realizzati.

Obiettivo principale di OAD è fornire reali e concrete indicazioni sugli attacchi ai sistemi informatici che possano essere di riferimento nazionale, autorevole e indipendente, per la sicurezza ICT in Italia e per l'analisi dei rischi ICT, necessaria anche per essere conformi alle normative sulla privacy.

Il passaparola è sempre lo strumento più efficace per promuovere l'indagine OAD, che in taluni casi "spaventa" la/il potenziale rispondente sia per certe domande un poco tecniche, sia, soprattutto, perché non si fida (ma questa volta a torto) del reale anonimato: e di conseguenza non ritiene opportuno far sapere che il suo sistema informatico, piccolo o grande che sia, è stato attaccato.

Si invitano pertanto tutti i lettori di questo articolo - lo da un lato a compilare il questionario, dall'altro a invitare i loro interlocutori di altre aziende/enti a compilarlo e a loro volta "passare parola". OAD garantisce totalmente l'anonimato della/del rispondente, e data la relativa generalità delle domande, non è possibile, in alcun modo, risalire all'azienda/ ente cui si fa riferimento.

Il questionario 2019 OAD

Dal 2018 l'indagine OAD individua 15 tipologie di attacchi digitali basate su che cosa viene attaccato, separandole il più chiaramente possibile dalle tecniche usate per portare l'attacco.

**Il Questionario 2019 OAD è online e accessibile,
ancora per poco, alla seguente pagina web:**

<https://www.oadweb.it/limesurvey/index.php/799974?lang=it>

Le prime sono relative agli attacchi rilevati per le 14 tipologie considerate, e con alcune delle loro più significative caratteristiche: frequenza nell'anno, tecniche di attacco usate, impatti subiti, tempi di ripristino nei casi più gravi. Qualora non fossero stati rilevati attacchi, o alcune tipologie di attacco, tutte le domande relative vengono saltate automaticamente dall'applicazione Web.

Il tempo richiesto per la compilazione del questionario dipende dal numero di diversi attacchi subiti, e dalle dimensioni e complessità del Sistema Informatico dell'azienda/ente della/del rispondente: tipicamente varia tra i 15 e i 30 minuti complessivi. Ma chi partecipa riceverà un significativo omaggio.

Un significativo omaggio a chi completa il Questionario 2019

La motivazione principale alla **corretta e veritiera compilazione** del questionario è il contribuire all'indagine che, unica in Italia, fornisce una **fotografia realistica del fenomeno degli attacchi digitali in Italia**, soprattutto per le piccole e piccolissime organizzazioni che costituiscono l'ossatura dell'economia italiana. Per ulteriormente spronare la/il potenziale rispondente a completare il questionario, OAD offre come piccolo **ringraziamento per il contributo** fornito ed i minuti spesi:

- Il numero di luglio 2019 della rivista mensile ISSA Journal, focalizzata sugli attacchi e sulle protezioni per i sistemi IoT, inclusi i droni dell'articolo di copertina;
- La recentissima ultima edizione del volume di 184 pagine, edito da Reportec, sulla sicurezza delle informazioni e la protezione dei dati.

Sponsor e patrocinatori

OAD è una iniziativa senza scopi di lucro, e le sponsorizzazioni servono solo a coprire una parte dei costi complessivi dell'intera iniziativa. È ancora possibile l'adesione di nuovi Sponsorizzatori e di nuovi Enti patrocinatori: i primi per coprire, almeno parzialmente, i costi dell'intera iniziativa OAD 2019, i secondi per allargare quanto più possibile sia ora il bacino di rispondenti, sia poi i lettori del rapporto finale.

Le Aziende e gli Enti che fossero interessati a considerare una sponsorizzazione di OAD 2019 possono direttamente contattare l'ideatore/realizzatore dell'indagine, inviando una e-mail a **m.bozzetti@aipsi.org**. La proposta di sponsorizzazione è scaricabile dall'allegato in fondo alla pagina web: **<https://www.oadweb.it/it/oad2019/oad-2019.html>**.

Analogamente, le Associazioni, anche di categoria, che fossero interessate a patrocinare OAD 2019 sono pregate di inviare quanto prima una e-mail di richiesta a **m.bozzetti@aipsi.org**.

2019

11 anni consecutivi di indagini via web sugli attacchi digitali intenzionali in Italia



ARROW UNIVERSITY 2019: CLOUD, IOT E UN BUSINESS DA RIPENSARE

Michele Puccio, Sales Director di Arrow ECS Italia, rinnova il successo della Arrow University 2019, spronando l'ampia platea *di Gaetano Di Blasio*

Oltre 450 i partecipanti attesi a Villa Quaranta di Pescantina per l'evento più importante organizzato dal distributore a valore aggiunto con sede a Bolzano.

Il recentemente nominato "padrone di casa", Michele Puccio, Sales Director di Arrow ECS Italia ha ampliato la formula tradizionale, aggiungendo un preludeo nel pomeriggio precedente la manifestazione. Si è trattato di un'occasione dedicata a incontri "uno a uno" tra vendor e partner, che sono stati apprezzati da tutti, permettendo di approfondire diverse tematiche e stringere rapporti di lavoro. Si è comunque mantenuta la formula degli appuntamenti tecnici e delle opportunità di networking.

Puccio ha, inoltre, provocato le diverse realtà del canale proponendo alcuni temi strategici sui modelli di business (in particolare sul modello "cliente - fornitore" che cambia, come da oltre un anno insistiamo con la nostra rivista Partners).

Innanzitutto il manager mette in guardia i partner: «Siete sicuri che il vostro modello di business sia coerente con il modello di business del cliente?». In questo modo esortando a sviluppare competenze sulle esigenze degli utenti finali con cui si lavora.

In tema di business model, Puccio evidenzia l'opportunità dei servizi, che si appoggiano al cloud e che si possono sviluppare attraverso piattaforme.

Queste aiutano a sviluppare i servizi, liberandosi dal "modello Amazon", con il prezzo al ribasso.

Un fronte molto promettente è quello dell'IoT, per il quale Arrow ha predisposto appositi kit, integrando l'offerta con la componentistica. In questo modo si indirizzano diversi "verticali" per fornire servizi.

A proposito dei servizi, Puccio ha sollevato la questione dei business ricorsivi basati sul modello degli abbonamenti, spronando ad adottarli nel B2B, dopo il successo ottenuto nel settore del consumer (con dalle "subscription" ai vari Netflix, Spotify e così via. Infine, il manager lancia un'ultima provocazione, sottolineando l'importanza di dedicare alcune risorse a studiare e sviluppare senza avere un obiettivo immediato. In un certo senso l'idea è quella di speculare sulle tecnologie e/o esigenze del futuro, in modo da essere pronti ad affrontare le prossime sfide.

Il tema dell'"intelligenza artificiale in primo piano, i cui prodomi sono una schiera di nuovi "autonomous thing".

«Siamo all'alba di una nuova "creazione"», afferma Puccio, prima di congedare la platea e dare il via ai workshop dell'Arrow University 2019, spingendosi a fare tre previsioni per l'immediato futuro:

1. Le acquisizioni nel mondo del canale continueranno per rispondere all'esigenze di soluzioni sempre più complesse;

2. Ci sarà il ritorno alla crescita delle marginalità, grazie a cloud e IoT, ma a patto che si impari a cavalcare i nuovi modelli di business;

3. Il cloud crescerà oltre il 50%.

L'obiettivo, conclude il manager, deve essere puntare sul valore, perché altrimenti vince il modello Amazon.



Michele Puccio, Sales Director di Arrow ECS Italia

I partner Platinum della Arrow University 2019

L'Arrow University è stata anche l'occasione per incontrare alcuni vendor, più precisamente i Platinum sponsor della manifestazione, tutti concordi dell'utilità di questa esperienza ed entusiasti delle nuove occasioni d'incontro e scambio, potendo presentare le ultime novità e altre "primizie".

Rocco Foti, Direttore Inside Sale di **Barracuda**, per esempio ha sottolineato l'interesse per le soluzioni di Network Security e Email Security, di grande attualità con la crescita dello spear phishing.

A fare la differenza, rivela in particolare Foti, è la specializzazione di Arrow e la capacità di comprendere a fondo le peculiarità del mercato, "il che ci ha permesso di crescere insieme". Anche trovando nuovi partner.



David Gubiani, Regional Director Sales Engineering EMEA Southern di **Checkpoint Software Technologies**, evidenzia alcune delle minacce, molte delle quali ricorrenti, ma sempre efficaci, che colpiscono le aziende, comprese quelle italiane.

Da sottolineare i rischi che si corrono pensando che il cloud sia la panacea per la sicurezza: «Il cloud provider si concentra sulla sicurezza dell'infrastruttura che è sotto la sua responsabilità, ma sono gli utenti che devono proteggere i propri dati all'interno del cloud» afferma Gubiani, avvertendo che ci sono molte novità presentate alla Arrow University.

Raffaella Zilli, Channel Account manager di **Trend micro** in Italia, ricorda la lunga collaborazione con il distributore basato a Bolzano, che li supporta, tra l'altro anche per la formazione e i POC, e sottolinea l'apprezzamento per la formula dell'Arrow University 2019, dove hanno portato soprattutto le soluzioni SCADA e quelle per il cloud. Soprattutto dove hanno siglato nuovi contratti.

Marco D'Elia, country manager di **Sophos** in Italia, illustra il nuovo assetto, studiato per gestire il canale, annunciando un ciclo di eventi per aumentare il recruitment di nuovi partner.

A Barbara Santamaria, Distribution Channel Team Leader di Sophos, spetta il compito di aiutare i partner a crescere "allargando" le loro competenze nella sicurezza per l'ondata di nuovi sistemi, come quelli autonomi.

Si accelera sul progetto Darwin facendo leva sulla soluzione Intercept X.

Luca Calindri, Country Sales Manager Italy & Malta

di **Thales**, ha il compito di illustrare il nuovo assetto societario, dopo la fusione con Gemalto, che ha razionalizzato le poche sovrapposizioni di prodotti, in attesa di un nuovo programma di canale che partirà dal primo trimestre 2020. In termini di go to market sono 100% canale e con Arrow da sempre.

Avranno un nuovo programma di canale dal primo trimestre 2020.

Pierpaolo Ali, Director Southern Europe Security, Risk & Governance di **Micro Focus**, evidenzia quanto sia importante la continuità del rapporto con Arrow per un'azienda che si rivolge al mercato enterprise.

Massimo Capobianco, Channel e Distribution Manager di **F5 Networks** in Italia, Con la Arrow University 2019 "festeggia" dieci anni di una manifestazione che «ha il pregio di raccogliere tanti partner», ottenendo un effetto moltiplicatore delle relazioni e del business.

Il focus tecnologico per F5 è centrato sulla sicurezza dell'identità e delle applicazioni, nuovo perimetro aziendale.

Come evidenziato da Capobianco, l'evento ha raccolto un nutrito numero di partner e vendor. Tra questi ultimi gli **sponsor Gold**: Citrix, CommVault, Infinidat e Symantec; gli **sponsor Silver**: Arrow Components, FireEye, Forcepoint, GFI Software, Huawei, Libraesva, Microsoft, MobileIron, Paessler, Praim, PulseSecure, Riverbed, RSA, Ruckus, Tenable e Tufin. A questi si aggiungono gli **Exhibitor**: Blancco, Carbon Black e McAfee. ❁

È disponibile il nuovo libro **CLOUD e MULTICLOUD**

CLOUD e MULTICLOUD

Piattaforme, servizi e applicazioni per la digital
transformation e un'azienda dinamica e competitiva

Giuseppe Saccardi

Reportec

Il libro è acquistabile al prezzo di 35 euro (IVA inclusa) richiedendolo a
info@reportec.it - tel 02 36580441 - fax 02 36580444

VISIBILITÀ, VELOCITÀ E COLLABORAZIONE CONTRO GLI ATTACCHI IT

X-Detection and Response di Trend Micro utilizza l'intelligenza artificiale per correlare i dati di endpoint, server, cloud e reti per abilitare visibilità e analisi dei rischi

di Giuseppe Saccardi

È tutta questione di velocità. Nella continua lotta tra attaccanti e difensori e in un periodo di profonda trasformazione dell'IT in progressiva migrazione verso il cloud, vince chi è più veloce. No, non si sta parlando di un verde campo di calcio, ma di un campo molto più critico, quello della sicurezza delle applicazioni e dei dati di business, e del problema di garantirne la protezione. E parlando di velocità viene spontaneo pensare ai circuiti automobilistici di Formula 1.

Oggi la security deve essere come un team di Formula 1, dove la condivisione e la raccolta complessiva di informazioni permette di mettere in pista una vettura performante. Questo grazie al fatto che ogni singolo pezzo è perfettamente integrato e progettato per fornire un miglior risultato complessivo.

"Il tutto è maggiore della somma delle singole parti", si potrebbe osservare contravvenendo a una stretta logica progettuale, e questo si può spiegare facilmente utilizzando un parallelismo con il mondo dei motori, osserva Gastone Nencini, Country Manager Trend Micro Italia.



*Gastone Nencini,
Country Manager
Trend Micro Italia*

Di certo il parallelismo ha una sua valenza. Quando un'automobile ha un problema o un guasto si può portarla dal carrozziere, dal meccanico o dall'elettroauto. Se per caso si rompe un finestrino o si buca una gomma ci sono altre figure professionali ancora che possono risolvere il problema.

È un approccio che prevede una specifica soluzione per il singolo problema. Ma non sempre è vincente, poiché non indaga a fondo il motivo di quanto accaduto, non ricerca la causa alla radice e non aiuta a prevenire altre criticità.

Per esempio, un fanale potrebbe essersi danneggiato a causa di sollecitazioni o vibrazioni troppo forti del veicolo e il problema potrebbe essere non nella lampadina, ma negli ammortizzatori. Se si cambia solo il fanale e non gli ammortizzatori, il problema è destinato a ripresentarsi.

Nella Formula 1 il modo di procedere è diverso e basato sul concetto di cooperazione a livello di team, con le singole parti che collaborano per ottenere un risultato superiore. Quando il veicolo ha un

problema, ma anche durante controlli di routine, una squadra di esperti lavora all'unisono dialogando. In prima battuta interviene la figura incaricata di analizzare la telemetria, che verifica tutti i parametri del veicolo. Successivamente questi dati vengono analizzati dagli esperti dei singoli ambiti che lavorano insieme per mettere l'auto nelle condizioni perfette. Si tratta in sostanza di un approccio orchestrato, volto ad abilitare a una strategia vincente. Le stesse differenze, mette in guardia Nencini, si possono ritrovare nelle aziende parlando di security, dove andrebbe adottata la stessa modalità di pensiero e strategia, ovvero passare da un approccio a compartimenti stagni fatto da singole soluzioni a una metodologia di azione orchestrata.

Il vulnus sta nel fatto che se oggi le infrastrutture IT sono molto evolute e complesse, purtroppo sono costituite in prevalenza da silos e questo è un rischio per l'intera organizzazione, perché la complessità aumenta le possibilità di subire un attacco e non risolverlo.

È anche possibile, se non del tutto probabile, che le varie parti dell'infrastruttura siano state create nel corso del tempo e in momenti diversi e ogni ambiente abbia una propria soluzione di security.

Il fattore critico è che molto spesso le soluzioni dei diversi ambienti non comunicano tra di loro e per i team di security raccogliere e analizzare i dati in silos è complicato e non permette alla struttura di reagire con la giusta reattività a eventuali attacchi. «In Trend Micro crediamo fermamente a una modalità di procedere corale, in grado di avere visibilità

sull'intera infrastruttura e risolvere e prevenire le criticità attraverso la collaborazione e l'identificazione delle cause alla radice, come in un team di Formula 1. Per questo abbiamo creato una soluzione che abbiamo chiamato XDR (X – Detection and Response), che potrebbe essere accostata alla telemetria del mondo dei motori. XDR utilizza infatti una sofisticata intelligenza artificiale per raccogliere e correlare i dati di email, endpoint, server, carichi di lavoro cloud e reti, offrendo visibilità e analisi altrimenti difficoltose o addirittura impossibili» ha commentato Nencini.

L'approccio adottato da Trend Micro si basa su un contesto più ampio che integra anche i dati dell'intelligence globale di Trend Micro e che permette di mettere in luce eventi che inizialmente possono apparire innocui, ma che possono essere indicatori di compromissione significativi e permettere di contenere rapidamente l'impatto riducendone al minimo gravità e portata.

Per semplificare il tutto una consolle con una sorgente di avvisi in ordine di priorità e ottimizzati, supportati da un'indagine guidata, semplifica poi le fasi necessarie per ottenere una comprensione in profondità del percorso degli attacchi e del loro impatto sull'organizzazione.

In questo modo si ha una prospettiva più ampia e un contesto migliore per identificare le minacce più semplicemente e contenerle in modo più efficace. Utilizzando un approccio di questo genere, osserva il manager, mettendo al centro la collaborazione e implementando la corretta soluzione, la security diventa così un gioco di squadra e l'azienda può continuare a sfrecciare veloce nel Gran Premio del Business, limitando al massimo le criticità. ❁

FORTICWP MIGLIORA LA SECURITY NEL CLOUD E NEL MULTICLOUD

La soluzione Fortinet è stata progettata per fornire un'ampia e esaustiva protezione del workload nel cloud e nel multicloud

di Giuseppe Saccardi

La mancanza di collaborazione nei diversi ambiti applicativi della sicurezza spesso comporta una scarsa visibilità centralizzata per quanto riguarda le attività di importanza critica.

Tra queste, le configurazioni di servizio, il traffico di rete, o gli eventi che riguardano la sicurezza e la data hygiene. È una sfida complicata dal fatto che oggi si ha a che fare con le diverse piattaforme dei provider di cloud pubblici.

Specificatamente per andare incontro alle problematiche delle aziende e supportarle nel rispondere a questa criticità, Fortinet ha annunciato FortiCWP, una soluzione dedicata alla protezione del workload del cloud che ha progettato per assicurare agli utenti il rispetto delle compliance e per diminuire i rischi associati alle applicazioni basate su IaaS.

In sostanza, FortiCWP permette alle aziende, osserva

Fortinet, di ottenere visibilità e controllo nella loro infrastruttura dinamica multi-cloud, essendo una soluzione di security posture management multi-cloud integrata e dinamica.

Integrazione con AWS, Google e Azure

Un aspetto chiave è che nativamente si integra con diverse infrastrutture cloud pubbliche, compreso l'utilizzo di API cloud-native di AWS, Google Cloud Platform e Microsoft Azure.

In questi contesti permette di rilevare le configurazioni, monitorare l'attività negli account cloud, analizzare e scansionare i dati, monitorare il traffico del cloud network e fornire report completi sulla compliance.

FortiCWP è poi integrata con i FortiGuard Labs, da cui riceve aggiornamenti sulla threat intelligence, e con FortiSandbox per analizzare i dati archiviati nel cloud ed identificare i contenuti malevoli.

I due servizi combinati permettono ai team che si occupano della sicurezza di disporre di visibilità e controllo degli eventi anche attraverso infrastrutture multi-cloud.

Una maggiore integrazione, visibilità e protezione la si ha utilizzando FortiCWP in combinazione con FortiGate-VM per la sicurezza del cloud (sia in ingresso che in uscita) e con FortiWeb per le applicazioni web e la protezione delle API. È infatti una combinazione che risponde alla necessità di mettere in sicurezza la rete, le applicazioni web e le piattaforme cloud.



È disponibile il nuovo libro **SMART & DIGITAL TRANSFORMATION**

SMART & DIGITAL TRANSFORMATION

Aziende, ambienti produttivi e città sono sempre più Smart, ma si deve garantire flessibilità, always-on, sicurezza e accesso al multicloud

Giuseppe Saccardi

Reportec

Il libro è acquistabile al prezzo di 35 euro (IVA inclusa) richiedendolo a
info@reportec.it - tel 02 36580441 - fax 02 36580444

CYBERARK ABILITA LA GESTIONE SAAS DEGLI ACCESSI PRIVILEGIATI

La soluzione SaaS CyberArk Privilege Cloud è stata resa disponibile sul marketplace di AWS

di Giuseppe Saccardi



CyberArk, azienda specializzata nello sviluppo di soluzioni di cyber security per la protezione degli accessi privilegiati, ha reso disponibile la sua offerta as-a-service CyberArk Privilege Cloud sul marketplace di Amazon Web Services (AWS). Va osservato che CyberArk Privilege Cloud è un'offerta SaaS che l'azienda ha sviluppato per permettere di proteggere, controllare e monitorare gli accessi privilegiati per infrastrutture on-premise, cloud e ibride.

La soluzione, ha evidenziato l'azienda, è progettata

per garantire una elevata sicurezza e per essere di ausilio alle organizzazioni nel gestire in modo efficiente le credenziali degli account privilegiati e i diritti di accesso, monitorare e controllare in modo proattivo le attività degli account privilegiati e rispondere rapidamente alle minacce.

Si tratta in pratica di una soluzione che permette di disporre di un livello ulteriore di sicurezza che non richiede la necessità di gestire infrastrutture extra on-premise, in modo che le organizzazioni possano concentrarsi sulle loro competenze principali.

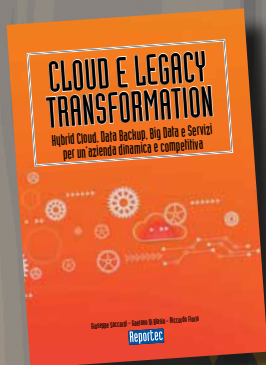
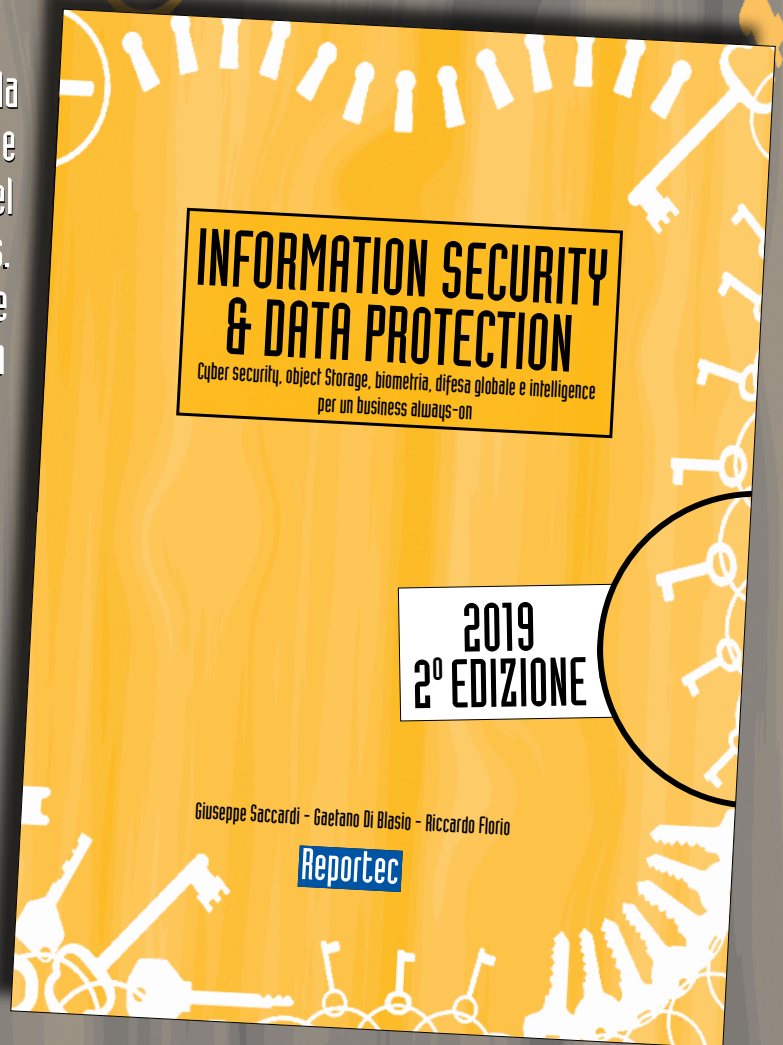
Come sviluppo, è la quarta soluzione di CyberArk a essere resa disponibile su AWS Marketplace, dopo Conjur Open Source, CyberArk Privileged Access Security Solution e CyberArk Privileged Access Security Solution for GovCloud, e conferma lo stretto rapporto di collaborazione esistente tra CyberArk e AWS.

Numerosi gli elementi di integrazione della soluzione con AWS e atti a rafforzare la sicurezza delle risorse cloud delle aziende, compresa l'integrazione con AWS Security Token Service (STS) e Amazon Inspector.

I clienti di CyberArk Privilege Cloud, ha spiegato la società, hanno anche la possibilità di scaricare la soluzione di onboarding AWS Automatic dal GitHub pubblico di CyberArk, che utilizza gli eventi AWS CloudWatch per rilevare le istanze EC2 appena create, registrarle automaticamente e gestirne gli account privilegiati. ❁

È disponibile il nuovo libro **SICUREZZA E PROTEZIONE DEI DATI**

In oltre 200 pagine il punto sulla situazione della cybersecurity e sulle dinamiche aziendali nella protezione del dato e della continuità del business. Una tematica sempre più vitale per le imprese, le quali devono mettere in conto che saranno attaccate. Ormai esistono sistemi automatici e pressioni da parte dei cybercriminali, tali per cui nessuno può sentirsi al sicuro: chi non è ancora stato attaccato lo sarà e, se non subirà danni gravi, sarà solo perché chi l'ha assalito cercava qualcos'altro.



È disponibili anche
CLOUD E LEGACY TRANSFORMATION

Il libro è acquistabile al prezzo di 30 euro (IVA inclusa) richiedendolo a
info@reportec.it - tel 02 36580441 - fax 02 36580444

CONSYS.IT DA 25 ANNI FORNISCE TRANQUILLITÀ ALLE IMPRESE

La società di consulenza e security advising ignora le proposte di acquisizione, cresce in Italia e lancia il progetto the Untold by Consys.it

di Giuseppe Saccardi

In un momento di transizione del mercato ICT italiano ci sono aziende che sanno fare la differenza. Tra queste Consys.it, che dal 1994 ha puntato sulle competenze e ha saputo crescere anticipando i cambiamenti del mercato. Marco Coppolino, fondatore e CTO di Consys.it insieme al CEO Alberto Fenini condivide la passione per il proprio lavoro nel pieno rispetto del proprio ruolo che si concretizza in una società dal taglio padronale con un modello enterprise, come enterprise sono i loro clienti.

Il successo di Consys.it nasce da questo e dalla capacità di stringere con i clienti una vera e propria partnership: quello che "vende" Consys.it non sono licenze, prodotti, soluzioni e/o o servizi per la sicurezza, ma "tranquillità". Spiega infatti Fenini, che il loro approccio consulenziale è multidisciplinare, il che permette di analizzare le esigenze del cliente da più punti di vista, ottenendo una visione più ampia e mirata. L'obiettivo, afferma il Ceo «è ottenere una visione analitica sulle aree d'intervento e un focus verticale integrato sulle aree d'intervento legate alla security nella sua completezza il tutto attraverso il

lavoro di un team di professionisti che aiutano i clienti a raggiungere gli obiettivi prefissati.».

Un approccio che oggi, con la digital transformation sta diventando una necessità, come da un anno circa continuiamo a predicare sulla nostra rivista Partners. La consulenza fornita da Consys.it fa leva sulle competenze maturate negli anni e sul continuo lavoro di formazione e scouting, anche in termini di soluzioni e nuove tecnologie. Poché sia Coppolino sia Fenini continuano a divertirsi facendo il proprio lavoro, le incessanti offerte per acquisire Consys.it la quale cresce più del mercato, a detta dei soci vengono sistematicamente rifiutate. Aumenta intanto la presenza sul territorio italiano, con l'espansione della sede d Roma, affidata a Vittorio Ranucci.

Inoltre, dopo un primo anno di "gestazione" prende piede il progetto the **Untold by Consys.it** avviato nel 2018 Da Coppolino e Fenini insieme a Edoardo Albizzati, che raccoglie i clienti svizzeri, quasi tutti del Canton Ticino, che diventa una sorta di laboratorio per studiare nuovi mercati e nuovi approcci e soluzioni.



*Da sinistra:
Vittorio
Ranucci,
Marco
Coppolino,
Alberto
Fenini,
Edoardo
Albizzati*



Fujitsu consiglia Windows 10 Pro.

Affidabile,
potente
e leggero

FUJITSU Notebook
LIFEBOOK U938

FUJITSU

shaping tomorrow with you



Sottile e ultra-mobile.
Il notebook Fujitsu LIFEBOOK U938 è per i
professionisti che desiderano il meglio, ovunque.

Windows 10 Pro | Intel® Core™ i7-8650U | 20 GB RAM

Info: www.fujitsu.com/it/ultrabook | Numero verde: 800 466 820
customerinfo.point@ts.fujitsu.com | blog.it.fujitsu.com

© Copyright 2019 Fujitsu Technology Solutions GmbH

Fujitsu, il logo Fujitsu e i marchi Fujitsu sono marchi di fabbrica o marchi registrati di Fujitsu Limited in Giappone e in altri paesi. Altri nomi di società, prodotti e servizi possono essere marchi di fabbrica o marchi registrati dei rispettivi proprietari e il loro uso da parte di terzi per scopi propri può violare i diritti di detti proprietari. I dati tecnici sono soggetti a modifica e la consegna è soggetta a disponibilità. Si esclude qualsiasi responsabilità sulla completezza, l'attualità o la correttezza di dati e illustrazioni. Le denominazioni possono essere marchi e / o diritti d'autore del rispettivo produttore, e il loro utilizzo da parte di terzi per scopi propri può violare i diritti di detto proprietario. Schermate simulate, soggette a modifica. App Windows Store vendute separatamente. La disponibilità di app e l'esperienza possono variare in base al mercato.

 Windows 10

Windows 10 Pro è sinonimo di business.