

COVER STORY

Gli approcci, i servizi, la condivisione, il Cyber Index in una chiacchierata con Hila Meller

pag. 8-11



IN QUESTO NUMERO:

CYBER ATTACK

pag. 12

Cyber security 2019
Trend Micro: nessuno è al sicuro

SOLUZIONI

pag. 14

- Askoll sceglie Check Point per la sicurezza mobile

pag. 16

- Micro Focus Fortify: codice protetto sin dall'inizio

pag. 18

- Nuovo programma di G Data per Managed service provider

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 47
gennaio 2019

Direttore responsabile:
Gaetano Di Blasio

In redazione:
Giuseppe Saccardi, Paola
Saccardi

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
Fax 02.36580444
www.reportec.it

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

Tutti i marchi sono
registrati e di proprietà
delle relative società

Copertina dedicata alla Cover story di BT, la cui vice president Security per l'Europa di BT, Hila Meller, ci "ospita" ai piani alti", da cui è possibile avere una visione privilegiata della cyber security a 360 gradi.

L'operatore di telecomunicazioni internazionale di origine britannica, infatti, è attivo in 180 paesi, gestendo una rete globale sulla quale passano un Terabyte di dati al secondo. All'interno di questi si registrano circa 600mila eventi di sicurezza, sempre ogni secondo.

Con Meller, Meller, che ci ha presentato il cyber index, uno strumento pubblicato sul sito di BT, abbiamo esplorato gli scenari disegnati dalle minacce vecchie e nuove e le strategie per gestire sicurezza e rischio.

Un altro punto di vista a tutto tondo sulla security si trova nella nostra rubrica sugli scenari del settore "Cyber Attack" ci è stato offerto da Trend Micro, uno dei vendor di sicurezza tra i più attivi nella cyber intelligence. Il Trend Micro Barcamp 2019, di Milano, ha fornito numerosi spunti e alcuni approfondimenti sulle minacce e gli approcci alla security. Oltre a Gastone Nencini, country manager di Trend Micro per l'Italia e a Myla Pilao, Director Technical Marketing di Trend Micro, hanno illustrato il loro punto di vista: Andrea Cavallini, Senior Cloud Developer & Security Champion - CCH di Tagetik, Antonio Fumagalli, UOC ICT dell'Azienda Socio Sanitaria Territoriale Papa Giovanni XXIII di Bergamo, e Alberto Meneghini, Managing Director di Accenture Security.

A chiudere le soluzioni e i casi di studio.

LE PRINCIPALI INDICAZIONI EMERSE DAL RAPPORTO OAD 2018

L'Osservatorio Attacchi Digitali in Italia traccia un quadro della situazione. Prefazione a cura di Nunzia Ciardi, Direttore Centrale Polizia Postale e delle Telecomunicazioni

L'Osservatorio Attacchi Digitali in Italia, OAD arriva nel 2018 al decimo anno di indagini sugli attacchi digitali in Italia. Il Rapporto OAD 2018 è realizzato dall'autore Marco R. A. Bozzetti con la sua società Malabo Srl, sotto l'egida di AIPSI, Capitolo italiano di ISSA, e con la preziosa e fattiva collaborazione dell'editore Reportec Srl e della Polizia Postale e delle Telecomunicazioni, che ha fornito i dati per il capitolo 11 e il cui Direttore Centrale, dott.ssa Nunzia Ciardi, ha scritto l'interessante prefazione. Il Rapporto OAD 2018 analizza gli attacchi intenzionali, rilevati nel 2016 e 2017 in Italia, ai sistemi informatici di organizzazioni di ogni dimensione e settore merceologico, incluse le Pubbliche Amministrazioni centrali e locali. Il Rapporto è costituito da 160 pagine A4, di cui 131 pagine per gli 11 Capitoli e 29 pagine per i 9 Allegati, che includono un glossario degli acronimi sulla sicurezza digitale, le presentazioni degli Sponsor, dei Patrocinatori e degli autori, l'illustrazione della metodologia seguita per l'impostazione del questionario sul web. L'indagine OAD 2018, rispetto alle edizioni precedenti,

ha ridefinito la tassonomia degli attacchi digitali, distinguendo chiaramente che cosa si attacca dal come si attacca, ossia con quali tecniche. Il questionario OAD 2018 per il 2016 ha solo chiesto che cosa è stato attaccato, mentre per il 2017 si sono approfonditi, per ogni tipo di attacco (il che cosa), le tecniche di attacco (il come), la loro frequenza, gli impatti, le motivazioni, il tempo di ripristino. Tra le tipologie di attacco l'indagine ha considerato anche i sistemi di automazione industriale, la robotica, i sistemi IoT, i sistemi basati su blockchain: le risposte raccolte sono indicatrici di come queste tecnologie si stanno estendendo in vari settori, e che siano attaccabili, come qualsiasi altro sistema ICT.

Il bacino di rispondenti emerso per l'indagine 2018 risulta costituito per la maggior parte da aziende appartenenti al settore ICT (36%), da quello dei servizi (13%) che include gli studi professionali, e da quello manifatturiero (13%), cui seguono con percentuali inferiori organizzazioni appartenenti a tutti gli altri settori merceologici (classificati secondo il codice ATECO), cui si aggiungono le Pubbliche Amministrazioni Centrali e Locali. Come dimensioni per numero di dipendenti, circa l'80% appartiene a organizzazioni fino a 250 persone, di cui il 37,5% a strutture fino a 10 dipendenti. Il campione emerso risulta quindi abbastanza ben bilanciato tra piccole strutture e quelle medio grandi, anche in riferimento alle ultime statistiche ISTAT che per le imprese rileva il 99,91% di PMI, e tra queste il 95,22% fino a 9 dipendenti

(si veda fig. 1). I compilatori del questionario 2018 sono stati 269, di cui il 20% è costituito da persone del vertice aziendale, il 19,22% dai responsabili dei sistemi informatici (CIO), il 17% da personale di terze parti cui è terziarizzata, in tutto o in parte, la gestione del sistema e della sua sicurezza, il 14% da personale appartenente all'unità organizzativa dei sistemi informatici. Solo per un 5,19% i responsabili della sicurezza informatica (CISO), con tale ruolo definito formalmente nell'organigramma.

Complessivamente gli attacchi rilevati nel 2016 hanno colpito il 41,57% dei sistemi informatici dei rispondenti, e nel 2017 il 45,32%. Tali percentuali sono in linea con quelle delle precedenti edizioni: prevalentemente attorno al 40%, pur avendo tale confronto un valore puramente indicativo e non statistico (si veda fig. 2), con un $\pm 3\%$ di varianza annua massima rispetto a questo valore. Dalla fig. 2 emerge chiaramente come il 2017 sia stato, con il 2008, uno degli anni con più attacchi digitali: OAI-OAD conferma quindi tutti i principali rapporti mondiali sugli attacchi digitali. Da tempo molti, soprattutto lato offerta cyber security, obiettano che il 40% è un valore è troppo basso, e che sicuramente molti attacchi non sono stati rilevati. Probabilmente è vero che molti attacchi subiti non sono stati rilevati: ma, a parte il furto di informazioni, altri tipi di attacchi, se non rilevati, significa che hanno avuto impatti trascurabili. Ma soprattutto, secondo l'autore, questo valore costante di attacchi nel tempo

dipende soprattutto dalle dimensioni troppo piccole della stragrande maggioranza delle aziende ed enti in Italia, come già evidenziato in fig. 1. Anche le circa 55.000 pubbliche amministrazioni centrali e locali sono prevalentemente costituite da piccole e piccolissime strutture, si pensi per esempio alle migliaia di piccoli comuni. Questa miriade di micro e nano imprese/enti non costituiscono il target per significativi guadagni illegali tramite specifici attacchi focalizzati. Possono essere oggetto di più semplice attacchi di massa o per "piccoli" guadagni (per esempio la diffusione negli ultimi anni di ransomware in Italia), o per attacchi con motivazioni di hactivism e/o di cyber terrorismo: attaccando contemporaneamente centinaia di migliaia di piccole imprese si possono causare gravi danni all'economia italiana.

Elemento chiave dell'indagine OAD è rilevare quali tipologie di attacco sono state le più diffuse tra i sistemi dei rispondenti:

- nel 2016: gli attacchi alle reti (44,62%), seguono il furto fisico di dispositivi ICT o di loro parti (33,33%) e gli attacchi ai propri sistemi terziarizzati (21,54%);
- nel 2017: gli attacchi al controllo degli accessi (39,39%), la saturazione delle risorse digitali (29,22%), la distruzione fisica di dispositivi ICT o di loro parti (28,57%).

La tecnica di attacco più diffusa e più usata considerando tutte le tipologie di attacco nel 2017 è quella che usa codici maligni, script e comandi diretti al

I più recenti dati ISTAT per le aziende:

- Fino a 9 dipendenti: 4.180.870
- Da 10 a 49: 184.098
- Da 50 a 249: 22.156
- 250 e più: 3.787

sistema operativo e/o alle banche dati. Segue, ma con largo distacco, l'uso di agenti autonomi (virus). Seguono con percentuali decrescenti i Toolkit, al terzo posto come diffusione. La raccolta di informazioni, tipicamente tramite social engineering, si posiziona come diffusione al penultimo posto, segno che buona parte degli attacchi nel 2017 è avvenuta soprattutto tramite strumenti tecnici e operando da remoto.

Oltre agli attacchi, OAD approfondisce quali misure di sicurezza, tecniche e organizzative sono adottate nei sistemi informatici dei rispondenti: come per gli anni precedenti, anche nell'indagine 2018 emerge che sistemi informatici dei rispondenti, indipendentemente dalle loro dimensioni e dai loro settori di appartenenza, risultano essere, nel complesso, nella fascia medio-alta per livelli di sicurezza e affidabilità, pur con vari punti di criticità, e con le misure organizzative in molti casi meno avanzate di quelle tecniche. Le principali caratteristiche della sicurezza digitale implementata dai rispondenti, con relative manchevolezze e criticità:

- a livello tecnico:

- » non buon bilanciamento tra le varie misure di sicurezza, mancando il più delle volte la definizione dell'architettura di sicurezza, anche se il 45,59% dei rispondenti afferma di disporre di architetture ad alta affidabilità;
- » limitate misure di sicurezza fisica per la protezione dei sistemi ICT soprattutto in locale per i sistemi dipartimentali;

- » autenticazione debole degli utenti, solo il 13% usa certificati e PKI;
- » per la protezione delle reti, metà circa dei rispondenti usa DMZ, 40% usa VPN, 1/3 usa filtraggi per le URL e ¼ usa IPS/IDS;
- » quasi il 20% ha un Piano di Business Continuity (continuità operativa) e il 33,84% un piano di Disaster Recovery, ma solo 1/3 di chi ha un piano di DR ha anche predisposto le risorse tecniche per attuarlo;
- » i sistemi operativi dei server sono in buona parte aggiornati alle più recenti versioni, e un 45,59% usa sistemi operativi "hypervisor" per la virtualizzazione dei server;
- » poco meno dei ¾ dei rispondenti usano housing, hosting e cloud per una parte o per l'intero sistema informatico;
- » il 94,46% usa anti-malware e antivirus, il 34,85% la sistematica gestione delle patch e delle versioni del software, solo il 32% circa i sistemi per l'archiviazione e la gestione dei log degli amministratori di sistema ;
- » a livello applicativo e dei dati trattati, solo il 16,67% effettua il controllo della sicurezza del codice per il software messo in produzione, dato che la maggior parte, soprattutto di PMI, utilizza applicazioni commerciali ritenute intrinsecamente sicure;
- » per ¼ circa dei rispondenti la gestione del sistema informatico è automatizzata.
- a livello organizzativo:
 - » nella maggior parte dei casi mancanza di definizione di chi deve occuparsi di sicurezza digitale;
 - » per 1/3 circa sono definite e in uso policy e procedure organizzative per la gestione della sicurezza digitale, ma meno del 10% ha definito



in esse una chiara separazione dei ruoli tra i diversi attori;

- » ancora scarso l'interesse sulle certificazioni professionali per la sicurezza digitale: il 40% circa delle aziende/enti rispondenti non è interessata e non richiede certificazioni né al proprio interno né ai fornitori ICT, e il 14,65% non sa addirittura rispondere in merito; sono più richieste certificazioni al proprio interno che ai fornitori;
- » la sensibilizzazione e la formazione degli utenti dei sistemi informatici sulla sicurezza digitale è ancora limitata e non sistematica.

Molto interessanti poi i dati forniti dalla Polizia Postale e delle Comunicazioni per il 2016-17, e analizzate nel capitolo 11 del Rapporto, che confermano l'incremento di attacchi nel 2017:

- nell'ambito della protezione delle Infrastrutture Critiche, gli attacchi rilevati sono aumentati del 22,27%, gli allarmi del 369%, le persone denunciate del 7,34%;
- nel contrasto al "financial cybercrime", le transazioni fraudolente bloccate in euro sono aumentate di quasi il 30%;
- nel contrasto al cyber terrorismo sono aumentate del 100% sia le persone denunciate che quelle arrestate.

Come indicato dalla dott.ssa Ciardi nella Prefazione al Rapporto, "tra le ragioni che favoriscono la diffusione della minaccia cyber, nei termini endemici attualmente sperimentati, figura la perdurante sottovalutazione degli aspetti legati alla sicurezza informatica, e il conseguente mancato approntamento di meccanismi adeguati di difesa tecnologica, sia da parte dei singoli cittadini, sia a livello delle piccole o grandi realtà aziendali e istituzionali del Paese". A giudizio dell'autore, la sottovalutazione della sicurezza digitale deriva principalmente dalla scarsa cultura digitale dei vertici e dei decisori di aziende/enti, sovente mal guidati da venditori e da consulenti di basso livello. Attuare le idonee misure di sicurezza digitale ha un costo non trascurabile, sovente non ritenuto giustificati da chi non ha subito attacchi e conseguenti impatti sul suo business/attività. Ma il venire attaccati non è un problema di se ma di quando: la sicurezza digitale costa, ma quanto costa la non sicurezza? *

Per scaricare il Rapporto 2018 OAD (gratuito):

- Registrarsi a <https://www.oadweb.it>
- Fornire il consenso esplicito privacy
- Scaricare il file in pdf



BT SI AFFACCIA SU UN PANORAMA PRIVILEGIATO DELLA SICUREZZA

Gli approcci, i servizi, la condivisione, il Cyber Index in una chiacchierata con Hila Meller

di Gaetano Di Blasio

BT è attiva in 180 paesi in cui fornisce servizi di telecomunicazioni, gestendo una rete globale sulla quale passano un Terabyte di dati al secondo. All'interno di questi si registrano circa 600mila eventi di sicurezza, sempre ogni secondo.

Si può senz'altro affermare che ciò conferisce all'operatore internazionale un punto di vista privilegiato sulla sicurezza.

A tal riguardo, evidenzia Hila Meller, vice president Security per l'Europa di BT: «La capacità di analizzare queste informazioni e offrire una cyber intelligence "operativa" è un nostro punto di forza, valorizzato dagli "insight" che possiamo produrre.

Una parte di queste informazioni sono direttamente disponibili sul sito di BT, dove viene pubblicato il "Cyber Index", che fornisce l'andamento delle minacce su base mensile, con uno scopo educativo per diffondere la cultura sulla sicurezza.

Un nuovo approccio alla difesa

Anche tra gli addetti ai lavori si riscontrano comportamenti superficiali. Per esempio, spiega Meller: «Ci si protegge dagli attacchi DDoS, ma non sempre si controlla accuratamente che la propria infrastruttura non sia utilizzata per generare attacchi di questo

Hila Meller, vice president Security per l'Europa di BT



tipo. Una maggiore conoscenza permette di ridurre il rischio dell' outbound DDoS»

L'esperta di BT sottolinea anche che cloud e IoT concorrono ad accrescere il perimetro da proteggere. Prima era interno all'azienda, mentre oggi è più ampio e, soprattutto più "fluidico".

Devono cambiare i sistemi di difesa continua Meller, infatti, sono oggi considerati più importanti controlli relativi alla gestione degli accessi, con le credenziali d'identità che acquisiscono un valore sempre maggiore.

Il Cyber Index fornisce informazioni che aiutano a comprendere le dinamiche, per esempio, al momento dell'intervista mostrava un evidente crescita di alcuni tipi di attacco, in particolare quelli sofisticati, che «sono probabilmente sponsorizzati da gruppi i quali hanno soldi, capacità e risorse da impegnare in questa attività certamente piuttosto onerosa», sostiene Meller.



Prepariamoci al primo cyber omicidio

La manager afferma inoltre, che nessuna organizzazione può sentirsi al sicuro: «C'è un disequilibrio, perché mentre ogni azienda deve essere pronta a difendersi da qualsiasi attacco per sentirsi protetta, i cyber criminali hanno bisogno che sia "colpito" un solo bersaglio per avere successo.

Nonostante il caso di Target risalente al 2014, che pure ha fatto scuola, gli esperti di BT hanno rilevato una crescita degli attacchi rivolti verso la supply chain, cioè attacchi che, invece di puntare direttamente sulla rete o sugli asset aziendali di un'impresa, trovano un punto debole nell'ecosistema. Il caso di Unicredit, risalente a un paio d'anni fa, pure ricade in questa categoria.

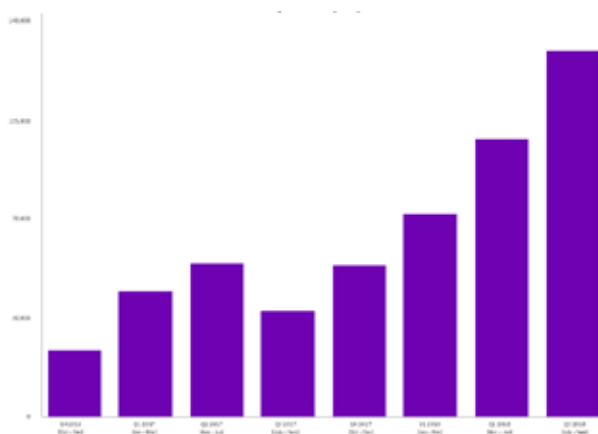
Crescono poi il phishing, lo Scam e i DDoS. Questi ultimi vedono aumentare notevolmente i volumi, grazie anche alla possibilità di acquistare DDoS as a service affittando così un "esercito" di bot.

Quello che preoccupa di più Meller è che, mentre

in passato gli attacchi cyber erano rivolti ai sistemi cyber, oggi si vedono più attacchi che hanno un impatto sul mondo fisico: «Il primo caso è stato il "vecchio" Stuxnet, ma gli esempi si differenziano: il blackout dell'aeroporto ucraino, gli hackeraggi dei sistemi per la guida delle automobili, le violazioni ai sistemi per la smart home. A essere a rischio sono anche le persone e, speriamo di no, ma potrebbe avvenire il primo caso di "cyber omicidio"».

Cyber Intelligence e l'approccio olistico di BT

Abbiamo chiesto alla vp security di BT se l'intelligenza artificiale può essere una soluzione per la sicurezza e, in effetti, scopriamo che BT sta usando da qualche anno l'artificial intelligence per individuare le minacce e gli attacchi, «ma l'AI da sola non è sufficiente, non ancora, almeno, anche per questo forniamo vari strumenti di analytics, in particolare graph analytics che aiutano gli esperti nell'interpretazione e nella correlazione fra diversi eventi»,



Andamento dello Scam via telefonia

spiega Meller, aggiungendo: «Occorre un approccio olistico che combina più metodi d'analisi: così si riesce a essere all'avanguardia».

Se torniamo ai 600mila eventi tracciati al secondo, di cui circa 120mila preludono a un attacco o sono prove di attacco, si osserva, continua l'esperta, che alcune minacce si riescono a bloccare velocemente e in modo anche automatico, mentre altre, poche, richiedono indagini approfondite.

«È interessante - prosegue Meller - che l'impatto sul nostro business di tutte queste prove di attacchi è minimo. Questo sia per le nostre capacità protettive, ma anche perché in BT abbiamo sviluppato un'ampia capacità di risk analysis».

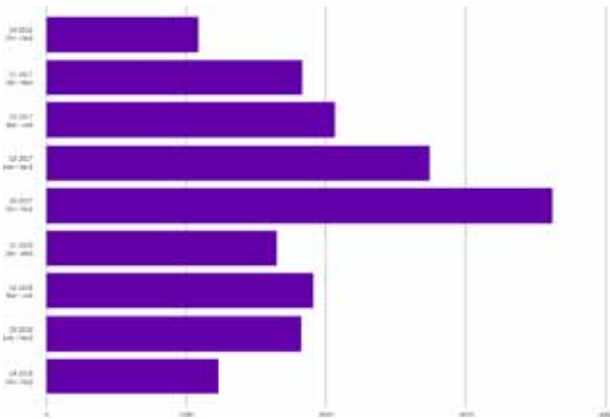
Il "segreto" l'analisi del rischio

Non è semplice identificare e quantificare il rischio, come dimostrano i tanti che ci provano senza successo. Afferma Meller: «Noi lo facciamo anticipando il rischio e, così l'impatto è zero sulla nostra Ebitda, (Earnings Before Interest, Taxes, Depreciation and Amortization), cioè il margine operativo lordo).

Questo è reso possibile dal nostro approccio olistico sulla sicurezza, che inizia con una buona integrazione della cyber security in diversi processi e termina con la presenza del responsabile di BT Security seduto al tavolo del consiglio di amministrazione». Un approccio di questo tipo è molto importante per la cyber resilience, che significa "saper assorbire i colpi" e si basa anche, evidenzia l'esperta, sulle molte attività di awareness, con corsi obbligatori, che tutti i dipendenti dell'azienda devono seguire, per esempio sul phishing.

Quello della sicurezza è un processo continuo e va gestito in quanto tale, perché il mondo delle minacce è molto dinamico, quindi occorre un'azione costantemente in evoluzione, rimarca Meller: «Ecco che, come accennato, monitoriamo sempre i rischi attraverso tutti gli strumenti necessari, comprese l'intelligenza artificiale e gli analytics. Inoltre, effettuiamo a rotazione in tutta l'azienda test di attacco contro noi stessi, con un team dedicato».

«La condivisione interna delle attività e dei risultati è fondamentale per avere la giusta "postura" ed



Andamento del Phishing

essere resilienti bloccando gli attacchi o annullando gli impatti negativi.

Tutto un insieme che comprende anche la collaborazione con enti preposti al controllo della sicurezza, come l'Interpol e altri sia a livello internazionale, sia locale, più precisamente con la Polizia Postale e delle telecomunicazioni», sottolinea la manager, che aggiunge: «Purtroppo c'è ancora troppa paura di denunciare una violazione informatica, mentre l'approccio corretto è quello che ci vede "tutti sulla stessa barca" e la condivisione, la fiducia, aiuta tutti, restando chiaro che una sicurezza al 100% è una chimera, ma un sistema resiliente ci consente di andare avanti a lavorare».

Anche il Cyber Index rientra nella logica della condivisione.

Del resto, il gruppo della sicurezza interna, Protect BT, è parte dello stesso gruppo che fornisce i servizi commerciali di sicurezza sul mercato.

Non a caso molti dei servizi che propongono sono nati per essere utilizzati dentro BT.

«È un punto di vista che porta naturalmente a una

condivisione dell'esperienza e del know-how, a beneficio di tutti. Un approccio che per BT è un vantaggio enorme.

Una maggiore esperienza serve anche per comprendere meglio i rischi, che, come su detto, è fondamentale. Soprattutto adesso che si parla sempre più di polizze assicurative per le violazioni informatiche, ma come si può scegliere un'assicurazione se non si conoscono i rischi che si corrono.

La carenza di esperti

Un grosso problema è la mancanza di persone con competenze sulla sicurezza. In BT affrontano la questione con diverse iniziative, a cominciare da un "riposizionamento", con corsi destinati a tecnici che aggiungono alle proprie nuove capacità. Si punta anche a stimolare gruppi generalmente trascurati, se non emarginati, magari per via dei soliti stereotipi: donne, disabili, autistici. Sono poi previsti programmi per neolaureati. ❁

CYBER SECURITY 2019 TREND MICRO: NESSUNO È AL SICURO

Un mondo interconnesso complica la lotta per la sicurezza, generando minacce pervasive e persistenti. Le previsioni a livello globale e in Italia. Cresce il social engineering

di Gaetano Di Blasio

L'appuntamento annuale con le previsioni del Trend Micro security Barcamp sulle minacce informatiche/digitali rivela un'ulteriore pressione sulla cyber security alimentata da un mondo digitale sempre più interconnesso.

Un mondo che sta perdendo la guerra contro il cyber crime e, più in generale, contro la sicurezza del digitale in tutti i settori economici. Ogni anno vengono scoperte 5 milioni di nuove minacce e la tendenza è in crescita, spiega Myla Pilao, director Technical Marketing di Trend Micro.

Sull'altro fronte, invece non si fa ancora abbastanza: sussiste un problema di formazione che sarebbe fondamentale per prevenire gli errori umani. Infatti, la Pilao aggiunge che l'83% delle minacce è veicolato dalle email. In particolare, Gastone Nencini, country manager di Trend Micro Italia, precisa che il proliferare di dispositivi e piattaforme, rende meno conveniente condurre attacchi

basati su exploit, a vantaggio del "vecchio" social engineering".

Già lo scorso anno si erano registrati molti attacchi BEC (Business Email compromise) e BPC (Business Process Compromise) e gli esperti di Trend Micro hanno misurato che dal 2015 gli Url di phishing bloccati da loro sono aumentati del 3.800%, mentre gli exploit kit sono diminuiti del 98%.

Intanto l'Italia risulta essere seconda in Europa per numero di malware individuati: 2.081.458, dietro la Francia, dove ne sono stati rilevati 2.446.859. Siamo poi 18esimi a livello mondiale e quarti in Europa in quanto a download di app malevole.

Attacchi con intelligenza artificiale

Gli attacchi BEC utilizzeranno sistemi di artificial intelligence per anticipare il comportamento dei manager, realizzando messaggi di phishing sempre più convincenti

Peraltro, gli attaccanti sfrutteranno anche tecnologie emergenti, come l'intelligenza artificiale, per anticipare i movimenti dei manager, mettendo a segno



*Myla Pilao, director
Technical Marketing di
Trend Micro*



Da sinistra, Alberto Meneghini, Antonio Fumagalli e Andrea Cavallini

attacchi BEC grazie a messaggi di phishing più convincenti.

Altri rischi riguarderanno la compromissione dei cellulari, più precisamente l'hackeraggio delle SIM, che consente di "dirottare" un cellulare senza che l'utente se ne accorga.

Aumenteranno le violazioni dei dispositivi casalinghi, man mano che crescerà il numero di apparati "smart home", in particolare se non si gestisce adeguatamente la loro sicurezza, cominciando con il cambiare la password di default del router.

Una cultura aziendale

Oltre al social engineering, le forme di attacco continueranno a sfruttare le vulnerabilità note, che in azienda restano non "ricucite" pure quando sono disponibili le patch. Si tratta di tattiche molto efficaci che saranno sempre più utilizzate anche per sfruttare vulnerabilità all'interno dei container.

Ciò anche se lo sviluppo del DevOps sta portando il software e la sua gestione all'attenzione dei business manager. La speranza è che cresca in azienda

la cultura della security by design.

Quest'ultima è una prassi fondamentale da implementare in ogni impresa, sostiene Andrea Cavallini, Senior Cloud Developer & Security Champion - CCH di Tagetik, ospite dell'evento insieme ad Antonio Fumagalli, UOC ICT dell'Azienda Socio Sanitaria Territoriale Papa Giovanni XXIII di Bergamo, e Alberto Meneghini, Managing Director di Accenture Security, tutti introdotti dalla Marketing manager di Trend Micro Italia, Lisa Dolcini.

Cavallini, in particolare, pone l'accento sui rischi del cloud evidenziati nel report di Trend Micro, laddove si sottolinea che "l'indebolimento delle misure di sicurezza nel cloud consentirà un maggior sfruttamento di account per il mining di cripto valute, portando a maggiori violazioni a causa dei sistemi mal configurati".

L'interconnessione vulnerabile

Nencini evidenzia la complessità generata dall'interconnessione di dispositivi, sistemi, software e modalità di utilizzo. Per esempio, afferma il country

manager, ci sono dispositivi che sono comandati in radio frequenza, come le gru per costruzioni, le quali possono essere manomesse e guidate da remoto o bloccate per chiedere un riscatto. Oppure, continua, si può manomettere una cassa per la riproduzione della musica collegata al WiFi.

«I dispositivi consumer non sono sicuri ma sono connessi con i dispositivi che portiamo a casa e usiamo per lavoro», avverte Nencini.

La complessità dell'interconnessione si coglie appieno grazie alla testimonianza di Fumagalli, il quale rivela quanti dati sono accompagnati ai paziente (ciascuno dei quali è mediamente collegato a 12 sistemi, dall'accettazione alla dimissione) e quanti altri sono correlati a diverse strutture fisse e mobili, dal badge del personale sanitario al sistema di tracciamento e identificazione di un carrello per i

medicinali, passando da un sistema di videosorveglianza o da quello che controlla la temperatura di un frigorifero e comprendendo tutto ciò che attiene alla conformità con la legge sulla privacy, GDPR incluso.

Gli attaccanti sfrutteranno anche tecnologie emergenti, come l'intelligenza artificiale, per anticipare i movimenti dei manager, mettendo a segno attacchi BEC grazie a messaggi di phishing più convincenti. Lo scambio, o l'hackeraggio di SIM, sarà una tecnica utilizzata per colpire gli utenti comuni. Questo metodo di attacco consente ai criminali di "dirottare" un cellulare senza che l'utente se ne accorga, rendendo difficile riprendere il controllo del proprio dispositivo. Inoltre, le smart home diventeranno un bersaglio sempre più attraente per gli attacchi che sfruttano router domestici e dispositivi connessi.

Ulteriori previsioni per il 2019 e maggiori dettagli

L'Italia si posiziona al 15esimo posto nella classifica delle nazioni colpite dagli attacchi BEC, destinati, come accennato, ad aumentare e divenire più efficaci, inoltre saranno destinati anche a dipendenti di minor grado. Eventi di cronaca, per esempio politici o sportivi, saranno utilizzati per attacchi di social engineering.

Le minacce alla democrazia cresceranno in termini di ingerenze propagandistiche e fake news. Danni collettari aumenteranno nei paesi che stanno addentrandosi nell'era digitale.

L'automazione verrà sfruttata per gli attacchi



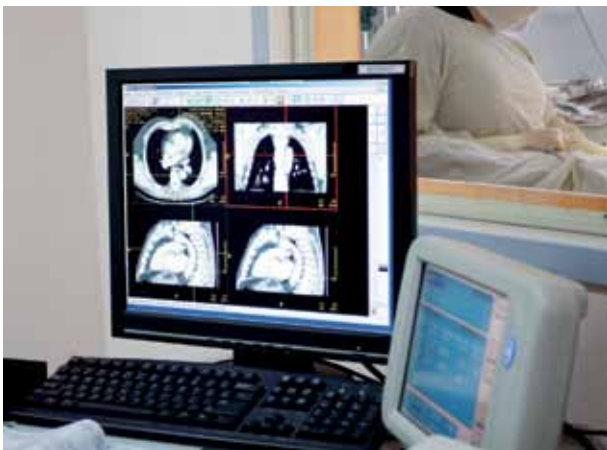
*Gastone Nencini,
country manager di
Trend Micro Italia*



Le smart home diventeranno un bersaglio sempre più attraente

I bug HMI saranno la prima fonte di vulnerabilità ICS per gli Industrial Control System

Infine, si prevede che ci saranno i primi casi di anziani vittime di attacchi ai dispositivi medici di tipo Smart Health



Business Process Compromise. Aumenteranno i casi di estorsione digitale, ma crescerà la supervisione in materia di cyber security.

Gli attacchi non si baseranno più sulle vulnerabilità 0-Day, impiegando invece strumenti di AI.

Cresceranno gli attacchi agli impianti industriali, sia di tipo SCADA, sia quelli che sfrutteranno i bug delle interfacce uomo-macchina: in particolare, i bug HMI

saranno la prima fonte di vulnerabilità ICS (Industrial Control System).

Infine, si prevede che ci saranno i primi casi di anziani vittime di attacchi ai dispositivi Smart Health. Le tecnologie per contrastare le minacce, però ci sono e stanno crescendo, occorre, come accennato all'inizio, accrescere la cultura della sicurezza e comprendere quali sono i rischi.

Il mondo ICT e gli esperti della sicurezza, almeno in buona parte sanno come realizzare dei risk assessment adeguati per definire i sistemi di contenimento delle violazioni, ma occorre che possano avere voce in capitolo: in altre parole, che un responsabile della sicurezza sieda nel consiglio d'amministrazione, in modo da collegare adeguatamente il rischio informatico a quello aziendale. ❁

ASKOLL SCEGLIE CHECK POINT PER LA SICUREZZA MOBILE

Gruppo Askoll ha implementato le soluzioni mobile Check Point Identity Awareness e Check Point (MTD) SandBlast Mobile

di Paola Saccardi

Le soluzioni di Check Point Software Technologies, fornitore di soluzioni di cybersecurity a livello globale, sono state selezionate per la protezione dei dispositivi mobile del Gruppo Askoll.

La necessità di Askoll era quella di garantire la protezione dei dispositivi mobili dei dipendenti in ogni luogo, prevenire le minacce alla sicurezza mobile e semplificare la gestione dei processi di sicurezza IT. Askoll è un'azienda italiana con 11 stabilimenti nel mondo e conta circa 2.000 dipendenti. È stata fondata nel 1978 da Elio Marioni per sviluppare la tecnologia sincrona applicata ai motori elettrici. Inizialmente sviluppata per il settore dell'acquariologia, questa tecnologia è stata in seguito estesa al mondo degli elettrodomestici. Dal 2015, il Gruppo è entrato nel mercato della mobilità sostenibile, divenendo produttore e distributore italiano di una gamma di veicoli elettrici Made in Italy.

In seguito al lancio sul mercato di una gamma di biciclette a pedalata assistita e dei suoi scooter elettrici, Askoll si è trovata davanti alla necessità di proteggere i propri dipendenti in maniera più efficiente ovunque si trovassero, pur garantendo loro la massima libertà operativa. «Abbiamo scelto la

tecnologia di Check Point Software Technologies, perché l'azienda ha un approccio alla sicurezza informatica in linea con il nostro, in grado di porre le persone davanti a tutto» ha spiegato Moreno Panetto, System IT manager di Askoll.

La soluzione per proteggere i dispositivi mobile

Askoll ha scelto di implementare le soluzioni mobile Check Point Identity Awareness e Check Point (MTD) SandBlast Mobile.

In particolare, Check Point Identity Awareness ha permesso al team IT guidato da Panetto di creare regole specifiche basate sull'identità. Questo ha portato a semplificare l'esperienza del personale addetto alla gestione IT, consentendo di proteggere gli utenti e ridurre il numero di regole richieste. La soluzione offre in pratica una visione dettagliata di utenti, gruppi e macchine, fornendo un controllo degli accessi e applicazioni senza precedenti attraverso policy precise basate sull'identità. La gestione e il monitoraggio centralizzati consentono di gestire le policy da un'unica console unificata.

«La soluzione Check Point Identity Awareness consente al personale di operare da svariate località in tutto il mondo, senza alcuna limitazione, mentre SandBlast Mobile garantisce la massima tranquillità, proteggendo i dispositivi dei nostri dipendenti da malware, applicazioni infette e minacce zero-day» ha commentato Panetto.



Check Point (MTD) SandBlast Mobile ha permesso all'azienda italiana di monitorare i dispositivi mobili e prevenire gli attacchi informatici, grazie alle proprie funzioni di protezione avanzate e alla visibilità. La soluzione protegge dalle minacce indirizzate a sistema operativo, app e rete, senza incidere sulle prestazioni o sull'esperienza utente. La versione 3.0 della soluzione inoltre prevede che la tecnologia threat prevention sia presente direttamente sul dispositivo.

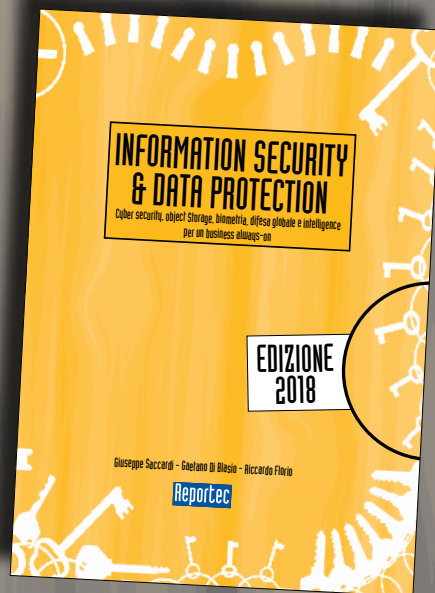
«Nel complesso, abbiamo conseguito una riduzione del 40% in termini di tempo e impegno utilizzati dal nostro team IT per gestire i problemi della sicurezza» ha concluso Panetto. ❁

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

MICRO FOCUS FORTIFY: CODICE PROTETTO SIN DALL'INIZIO

Attraverso la famiglia Fortify, Micro Focus propone un modello dinamico di sicurezza che protegge il codice sia in fase di sviluppo sia, una volta entrato in produzione, in condizioni statiche e dinamiche

di Riccardo Florio

Le applicazioni rappresentano il nuovo campo di battaglia nella lotta contro il crimine informatico, tanto che gli analisti stimano che oltre l'80% delle applicazioni open source e commerciali presenti vulnerabilità di sicurezza con implicazioni serie per la gestione dei dati privati. Se le applicazioni Web sono una fonte di rischio significativa per le organizzazioni, quelle mobili presentano rischi ancora maggiori

Qualsiasi tipo di software, sia sviluppato internamente sia acquisito commercialmente, presenta vulnerabilità e, in assenza di un approccio indirizzato al Software Development Life Cycle (SDLC) è probabile che applicazioni vulnerabili siano rilasciate in produzione o che lo risultino a un certo istante della loro vita.

Il processo di integrare la sicurezza all'interno del ciclo di sviluppo del software è noto come Software Security Assurance (SSA) e si concretizza attraverso tre approcci complementari:

- l'analisi statica del codice,

- il test dinamico della sicurezza delle applicazioni,
- la predisposizione di tecnologie di Runtime Application Self-Protection (RASP).

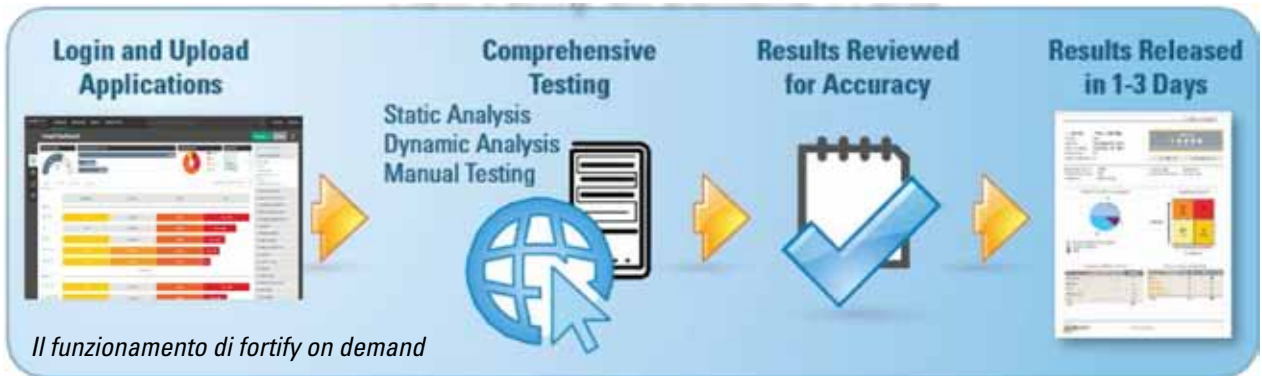
Per rispondere puntualmente a ciascuna di queste esigenze e predisporre un modello SSA Micro Focus ha predisposto la famiglia di soluzioni Fortify.

Le soluzioni Fortify per un codice sicuro

Le soluzioni Fortify predispongono un approccio proattivo di Software Security Assurance per affrontare in modo sistematico il rischio di vulnerabilità nel software sulla base del principio che è più efficace e conveniente proteggere le applicazioni mentre sono in fase di sviluppo che farlo dopo che sono state rilasciate.

Il modello di protezione Fortify ruota attorno a tre fasi: assessment, Security Assurance e difesa attiva sfruttando le tecnologie RASP (Runtime Application Self Protection) pensate per rendere le applicazioni intrinsecamente sicure a partire dalla fase di sviluppo.

Attraverso la piattaforma Fortify Software Security Center (SSC) gli utenti possono rivedere, controllare, definire priorità e gestire le attività di "remediation", tenere traccia dei test di sicurezza eseguiti sul software e misurare i miglioramenti tramite un dashboard di gestione e report.



Fortify Application Defender: le applicazioni si difendono da sole

Fortify Application Defender è una soluzione RASP che fornisce visibilità centralizzata sull'utilizzo e l'eventuale abuso di un'applicazione proteggendola in tempo reale dai tentativi di sfruttamento delle vulnerabilità e da altri tipi di violazioni. La protezione RASP è, infatti, capace di analizzare il codice in tempo reale all'interno dell'ambiente di produzione e di attuare contromisure sulla base dei risultati. Application Defender può essere implementata come soluzione on-premise oppure sottoscritta come servizio; è caratterizzata da un processo di installazione estremamente semplice e richiede solo pochi minuti per diventare operativa.

Fortify Static Code Analyzer (SCA) e WebInspect

Attraverso una serie di algoritmi e una base di conoscenza estesa di regole di codifica sicure, Fortify SCA analizza il codice sorgente di un'applicazione alla ricerca di vulnerabilità che potrebbero essere sfruttate in applicazioni distribuite. Fortify SCA prevede opzioni di implementazione flessibili con possibilità di accesso on-premise oppure on-demand. Fortify WebInspect imita le tecniche di hacking e gli attacchi, consentendo di analizzare a fondo le

applicazioni e i servizi Web per individuare possibili vulnerabilità di sicurezza. WebInspect consente di testare le applicazioni Web dallo sviluppo alla produzione, di gestire in modo efficiente i risultati dei test e favorisce la distribuzione di conoscenza sulla sicurezza all'interno dell'azienda.

Test dinamico per ogni tipo di applicazione

Fortify on Demand (FoD) è il servizio di Testing as a Service (TaaS) per controllare il livello di sicurezza del software senza richiedere l'acquisto di alcun hardware né l'installazione di alcun software e che supporta applicazioni sia sviluppate internamente sia da terze parti e commerciali.

FoD è disponibile per assessment sia statici basati sulla soluzione Fortify Static Code Analyzer oppure dinamici alimentati da WebInspect.

Combina l'attività di test automatico con una metodologia di test manuale svolta da un gruppo di "application penetration tester" che imita le tecniche di attacco dei cyber criminali sull'applicazione Web. Fortify on Demand estende i test anche alle applicazioni mobili prendendo in considerazione i tre livelli che costituiscono lo "stack" tecnologico: client, rete e server. Tramite l'integrabilità con Application Defender è possibile creare e gestire la protezione dalle vulnerabilità individuate durante la fase di "remediation". ✱

NUOVO PROGRAMMA DI G DATA PER MANAGED SERVICE PROVIDER

Soluzioni e servizi per una sicurezza “armonica” e intelligente, erogata in cloud e gestita dal canale. Premio innovazione all’assicurazione con Reale Mutua e Margas

di Gaetano Di Blasio

GData ha sempre cercato di indirizzare il proprio canale laddove si manifestano le esigenze. Negli anni scorsi il vendor d’origine tedesca ha investito per consentire al proprio canale di accrescere le competenze di settore, anche al fine di aiutare i clienti a realizzare progetti sicuri. Oggi prepara i partner a scalare di livello per crescere sulla scala del valore, proponendo servizi gestiti.

Come più volte abbiamo affermato, le imprese del canale devono stringere una vera e propria partnership con quelli che fino a ieri consideravano “semplici” clienti. Fornire servizi gestiti, quasi operando come “reparto interno” è il passo più critico per il successo futuro.

I partner di G Data dovranno comunque impegnarsi in nuova formazione, anche perché crescono le vendite di prodotti e soluzioni nuove, come il modulo di Patch Management aggiuntivo per G Data Endpoint Protection e integrato in G Data Total Control, che è stato tra i prodotti più venduti dell’ultimo anno, ma che prelude a una serie di novità pronte a soddisfare

le esigenze indotte dal cloud, dove tutto si vuole sia “as a service”, dal desktop alle applicazioni alle piattaforme.

Esigenze che non tutti i partner sono già preparati a soddisfare, ci spiega Paola Carnevale, Sales & Channel Director di G Data Italia, la quale aggiunge: « La nostra missione, come vendor che fa della propria vicinanza al mercato una vera e propria strategia, è quella di proporre al canale strumenti per rispondere a queste esigenze».

In Smau, dunque, G Data ha lanciato un programma studiato appositamente per i partner che intendono rispondere a queste esigenze. In particolare questo sarebbe possibile con la soluzione G Data Managed Endpoint Security, che, afferma Carnevale: « si è rivelato il prodotto più ricercato dagli operatori di canale che desiderano accedere al mercato dei servizi gestiti erogati via cloud e pure dagli MSSP intenzionati a completare il proprio portafoglio servizi». Un programma che non riguarda le solite logiche legate a certificazioni e listini, ma fornisce strumenti per alimentare la crescita, ridefinendo la supply chain per rendere più armonico il modello di ecosistema.

Inoltre, pure per promuovere il programma, con le prossime, release sarà resa multitenant la console di gestione delle soluzioni business G Data tradizionali.

Diverse le novità di prodotto, tra cui, in particolare, un’assicurazione, elemento sempre più apprezzato



*Giulio Vada,
country manager di
G Data Italia*



*Paola Carnevale,
Sales & Channel
Director di G Data
Italia*

dalle aziende, a cominciare dalle piccole e medie, ma non solo.

È motivo d'orgoglio per Giulio Vada, country manager di G Data Italia, poiché la polizza "Privacy & CyberRisk", realizzata grazie alla collaborazione con Reale Mutua e il Broker Margas, ha ottenuto il premio innovazione in Smau.

Al riguardo, il manager italiano commenta: «Questo premio conferma la bontà della proposta di sostegno alle PMI nell'azzeramento dell'impatto economico di eventuali rischi residui in termini di tutela dei dati».

Le soluzioni analitiche

Tornando alle novità tecnologiche presentate da G Data nel corso del 2018 e a quelle preannunciate per il 2019, Vada evidenzia: «Nel corso dell'anno abbiamo potenziato notevolmente le tecnologie analitiche al servizio della clientela G Data. Per esempio, negli scorsi mesi abbiamo bloccato l'11,6% dei tentativi di infezione con malware non noti su scala globale con il solo impiego dei nostri nuovi

strumenti NGAV (Next Generation Anti Virus), tra cui Filecloud e Behaviour Blocker».

Si tratta di parti integranti del rilevamento euristico dei software malevoli, che, grazie al sistema di machine learning realizzato da G Data, «contribuisce a determinare quali caratteristiche in quale combinazione e ponderazione danno luogo all'identificazione di una minaccia zero-day come tale», spiega Vada, che continua: «I nostri clienti beneficiano così, di un livello di protezione superiore, ma grazie ai nuovi processi che saranno implementati nelle release dei prodotti consumer e business nel corso del primo semestre 2019, integreremo funzioni aggiuntive particolarmente innovative».

Infine, sono previste novità in tema di soluzioni per ambienti virtualizzati, a completamento delle piattaforme ha disposizione del canale. ❖