Comunicato stampa

Aggiungi valore.
Ispira fiducia.

29 gennaio 2019

TÜV SÜD: i 9 trend della Cybersecurity per il 2019

Milano. Digitalizzazione sempre più spinta e crescente connettività fornita dall'Internet of Things (IoT) offrono enormi opportunità di business ma anche rischi imprevedibili e gravi vulnerabilità. Tali vulnerabilità possono poi essere sfruttate dalla criminalità informatica per ricavarne dei benefici economici.
TÜV SÜD, ente di certificazione che opera a livello globale, illustra 9 tra le più rilevanti minacce legate alla cybersecurity a cui le aziende dovrebbero fare attenzione nel 2019 e presenta un tool specifico, tramite TÜV Italia, per ottemperare correttamente al GDPR.

Lo scenario che il rapporto del Clusit fornisce è preoccupante. In Italia nei soli primi sei mesi del 2018 i cyber attacchi sono cresciuti del 31% rispetto all'anno precedente (fonte: Clusit https://clusit.it/rapporto-clusit/).

Tutte le organizzazioni che ancora non hanno fatto propria la cultura dell'importanza della gestione dei dati, ancor più se legati a comportamenti individuali, sono un obiettivo sensibile per i cyber criminali.

"I criminali informatici stanno rapidamente sviluppando e adottando nuove forme di attacco per hackerare reti di aziende e infrastrutture critiche. Diventa, pertanto, sempre più importante continuare ad investire in cyber security per stare al passo con lo sviluppo tecnologico", afferma Andy Schweiger, Managing Director di Cyber Security Services di TÜV SÜD. "TÜV SÜD è un partner indipendente che offre le competenze tecniche necessarie e aiuta i clienti a sfruttare le opportunità offerte dalla digitalizzazione."

Secondo TÜV SÜD, i trend da monitorare nel 2019 sono:

1 - Protezione dei dati e GDPR: buona la prima!
L'attuazione del regolamento generale sulla protezione dei dati dell'UE (GDPR), che è entrato in vigore il 25 maggio 2018, rappresenta ancora una grande sfida per molte aziende. Dopo le prime multe

comminate a novembre 2018, le aziende stanno affrontando una crescente pressione per aumentare gli investimenti nella propria sicurezza IT. Invece di effettuare audit isolati sulla protezione dei dati e basati su interviste, vanno adottate richieste di monitoraggio integrate per un approccio sistematico. Una corretta politica di protezione dei dati necessita di costanti investimenti nella Sicurezza IT. TÜV Italia, in particolare, promuove un servizio di consulenza personalizzata supportato da un tool per guidare le aziende all'osservanza degli adempimenti richiesti dalla normativa in tema GDPR. Il tool ha come obiettivo di supportare le organizzazioni nel controllo sui propri sistemi IT e permette di dimostrate che l'azienda ha adottato adeguate misure tecniche ed organizzative a tutela dei cyber crime.

2 - Ingegneria sociale: le persone sono l'anello più debole

Molte aziende utilizzano sofisticate tecnologie, come servizi di intelligence sui rischi e penetration test, per identificare le vulnerabilità IT, ma trascurano la formazione del personale. L'ingegneria sociale è da tempo diventata un'arma standard nell'arsenale a disposizione di ogni criminale informatico come, ad esempio, "La frode del CEO", basata su email di phishing fasulle ma realistiche da parte del top management che ingannano i dipendenti. Le truffe di Social Engineeing sono relativamente facili da creare e continueranno ad aumentare nel corso del 2019.
Informazioni specifiche, addestramento e formazione dedicata, come quelle offerte da TÜV SÜD, aiutano a mitigare questo rischio.

3 - L'incremento del fenomeno noto come "Shadow IT": è necessario staccare la spina

Gli investimenti in ambito IT o le acquisizioni aziendali rappresentano progetti complessi e spesso molto impegnativi, in cui le aziende dimenticano frequentemente di disconnettere apparecchiature obsolete o non più necessarie. Funzionando su sistemi operativi non supportati e patch di sicurezza mancanti, queste apparecchiature datate e/o non ufficiali, note come "shadow IT", offrono ai criminali informatici delle comode falle da utilizzare per hackerare le reti aziendali. I rischi possono essere però minimizzati monitorando continuamente la sicurezza dell'infrastruttura IT e dismettendole.

4 - Fabbriche intelligenti: integrare la sicurezza fin dal principio

Per sfruttare le opportunità offerte dall'Industrial Internet of Things (IIoT), le aziende investono in impianti di produzione connessi. La sicurezza dovrebbe essere integrata in questo processo fin dall'inizio, poiché la successiva protezione degli elementi o macchinari connessi contro gli attacchi informatici è un processo complesso e costoso. Analisi di vulnerabilità e valutazioni approfondite sulla sicurezza, come quelle offerte da TÜV SÜD, aiutano le aziende a verificare lo stato di sicurezza dei loro impianti industriali.

5 - Superare le barriere linguistiche: promuovere la comunicazione tra esperti e dirigenti

Sempre più aziende stanno portando il tema della sicurezza informatica ai più alti livelli di gestione. È dunque evidente che la sicurezza informatica stia diventando un tema centrale non solo per i responsabili IT ma anche per la gestione del business operativo da parte del management. Tuttavia, i dirigenti e gli esperti IT parlano spesso lingue diverse e adottano prospettive molto differenti su molte questioni. In questo caso trovare un linguaggio comune e comprensibile è molto utile per evitare fraintendimenti e dunque ritardi negli investimenti necessari per la sicurezza IT.

6 – Cryptomining vs. ransomware: prestare maggiore attenzione al mining

Secondo Bitkom, l'associazione dell'industria tecnologica tedesca, nel 2016 e nel 2017 si sono verificate perdite, causate dai malware, fino a 43 miliardi di euro a danno di sole società tedesche. Nel 2019 gli esperti si aspettano una più marcata tendenza al cryptomining. Anziché danneggiare o rubare dati, il cryptomining utilizza l'infrastruttura IT dell'azienda per effettuare l'estrazione intensiva a livello della CPU (Unità Centrale di Elaborazione) di cripto valute, senza che il proprietario dell'infrastruttura se ne accorga. La Security by Design, che considera i requisiti di sicurezza per software e hardware fin dalla fase di progettazione e sviluppo, è una possibile soluzione per evitare in seguito lacune nell'ambito della sicurezza.

7 - Anche i criminali informatici usano l'intelligenza artificiale

Gli attacchi informatici si basano sempre più spesso sui principi di machine learning e intelligenza artificiale. La corrispondenza dei pattern, ovvero il controllo dei valori rispetto a pattern noti, non basta più per evitare questi attacchi. Le aziende infatti dovrebbero concentrarsi sull'identificazione delle anomalie e utilizzare l'intelligenza artificiale (AI) per la sicurezza informatica. Grazie a questo approccio sono in grado di identificare precocemente attività anomale.

8 - Sicurezza del cloud: crittografia sicura

Secondo un sondaggio di Bitkom, il 57% degli amministratori delegati e dei responsabili IT intervistati ha dichiarato di considerare "sicura" o "relativamente sicura" l'archiviazione dei dati aziendali nel cloud pubblico. Lo storage crittografato nel cloud, come quello offerto da TÜV SÜD e dalla sua controllata Uniscon, è la soluzione che offre il massimo livello di sicurezza e conformità alle normative sulla protezione dei dati. Il trasferimento e l'archiviazione dei dati sono crittografati e non è possibile accedervi, nemmeno da parte del fornitore di cloud servizi.

9 - Attacchi a livello governativo

Gli attacchi informatici professionali su larga scala lanciati dagli hacker che lavorano per un governo continueranno a crescere nel 2019. Per questo il paese di origine del fornitore dovrebbe essere un elemento fondamentale nelle decisioni di acquisto di un software di sicurezza informatica. In qualità di partner terzo, TÜV SÜD supporta le aziende nella ricerca della migliore soluzione possibile.

Ulteriori informazioni sui servizi di cyber security sono disponibili su https://www.tuv-sud.com/industries/digital-it-services

Maggiori informazioni sul tool GDPR sono in questa pagina: https://www.tuv.it/it-it/attivita/servizi-customizzati-la-soluzione-di-tuev-italia/compliance-aziendale/applicativo-gdpr-di-tuev-italia-in-regola-con-gli-adempimenti-per-garantire-la-compliance-aziendale

Corsi sulla sicurezza informatica offerti da TÜV Italia Akademie sono disponibili alla pagina:
https://www.tuv.it/it-it/attivita/tuev-italia-akademie/catalogo/ict
https://www.tuv.it/it-it/attivita/tuev-italia-akademie/catalogo/privacy
I corsi possono anche essere progettati su misura in funzione delle esigenze aziendali.

Contatti con la stampa:

Sabrina Zapperi – Emilia Pistone Communication TÜV Italia – Gruppo TÜV SÜD Tel. +39 24130-1 sabrina.zapperi@tuv.it – emilia.pistone@tuv.it Internet: www.tuv.it	Ufficio stampa TÜV Italia Sangalli Marketing & Communications Michela Sangalli – msangalli@sangallimc.it Federico Maggioni – fmaggioni@sangallimc.it Tel. 0289056404

Click here to enter text.