Gli Specialisti Italiani della Cyber Security

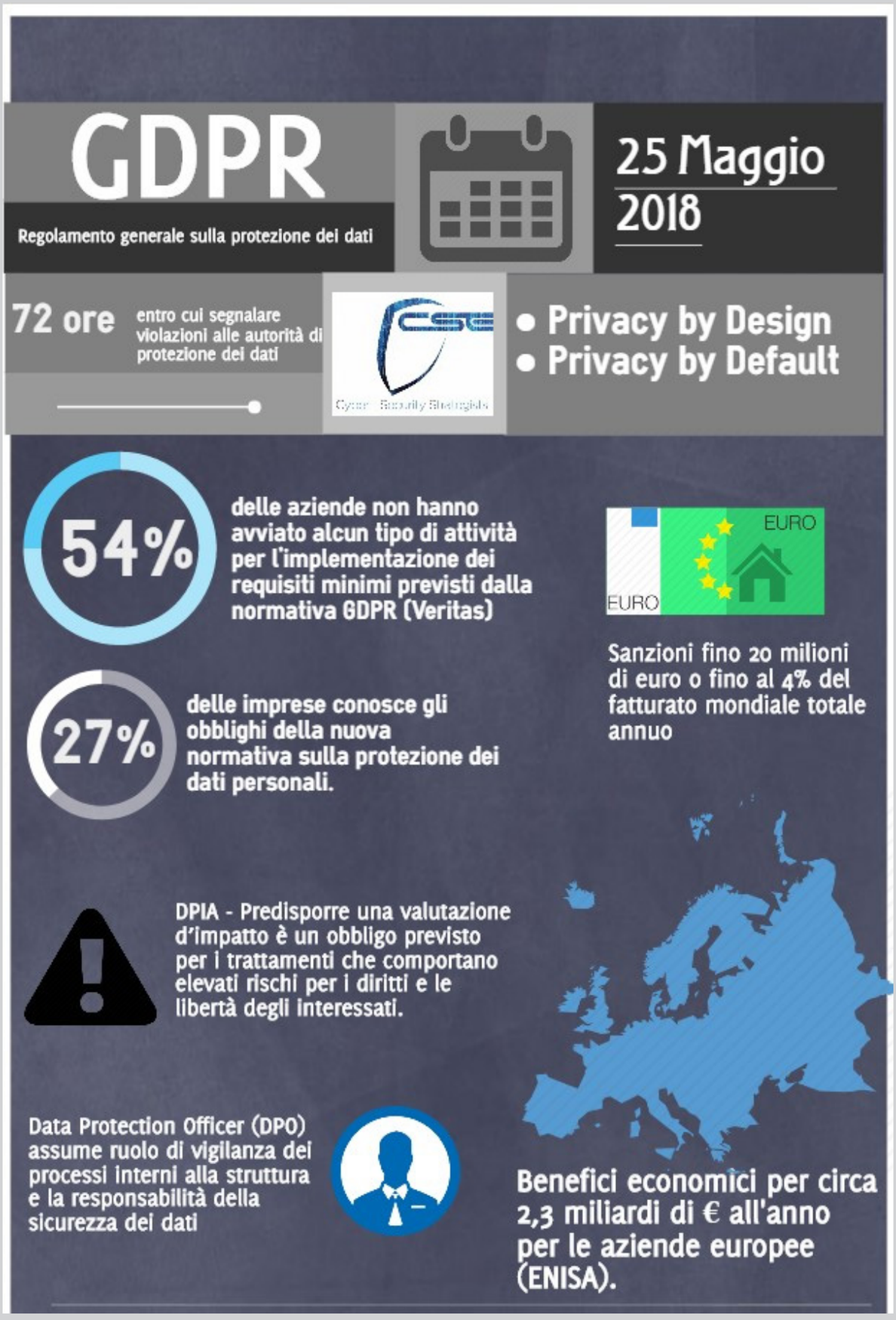
2018 Threat Landscape
Uno sguardo al futuro

Quali sono i fenomeni e gli eventi che caratterizzeranno il panorama della cyber security nei prossimi dodici mesi?
Quali saranno le ricadute in termini economici per le nostre imprese?

Per fornire utili risposte è necessario valutare con attenzione tutti gli eventi occorsi negli scorsi anni cercando di immaginare come attori malevoli possano beneficiare dell'attuale scenario tecnologico e della sua rapida evoluzione. Non solo, occorre tener presente i nuovi regolamenti internazionali in ambito privacy e cyber security ed ovviamente non si può prescindere da una analisi geopolitica di ciascun fenomeno.
Vediamo quali sono i principali aspetti critici con i quali ci confronteremo nel 2018.

I GDPR: molte aziende non saranno conformi al nuovo regolamento UE

Uno dei principali eventi del 2018 è l'attuazione del Regolamento generale per la protezione dei dati personali n. 2016/679 (General Data Protection Regulation o GDPR) ovvero la normativa di riforma della legislazione europea in materia di protezione dei dati.
Il regolamento è destinato ad introdurre cambiamenti in tutti i processi aziendali, per questo motivo è auspicabile che ciascuna impresa si sia mossa per tempo per garantire la conformità normativa. Il GDPR nasce con l'intento di armonizzare le leggi sulla privacy dei dati in tutta Europa e proteggere i cittadini dell'UE. Tutti siamo al corrente del potenziale impatto economico delle sanzioni previste in caso di non conformità, (4% del fatturato globale annuale, o sanzione fino a 20.000.000 euro per inadempienza), in pochi considerano la sospensione permanente dell'autorizzazione al trattamento dei dati che potrebbe determinare l'interruzione dell'attività di un'azienda. Una volta che la legislazione GDPR sarà esecutiva, qualsiasi violazione dei dati personali che abbia un impatto sui cittadini dell'Unione europea dovrà essere segnalata entro 72 ore. Il GDPR vuole fornire trasparenza ai titolari dei dati sul modo in cui le loro informazioni vengono raccolte e utilizzate.


GDPR
Regolamento generale sulla protezione dei dati
25 Maggio 2018
72 ore
entro cui segnalare violazioni alle autorità di protezione dei dati
• Privacy by Design
• Privacy by Default
54%
delle aziende non hanno avviato alcun tipo di attività per l'implementazione dei requisiti minimi previsti dalla normativa GDPR (Veritas)
EURO
EURO
Sanzioni fino 20 milioni di euro o fino al 4% del fatturato mondiale totale annuo
27%
delle imprese conosce gli obblighi della nuova normativa sulla protezione dei dati personali.
DPIA - Predisporre una valutazione d'impatto è un obbligo previsto per i trattamenti che comportano elevati rischi per i diritti e le libertà degli interessati.
Data Protection Officer (DPO) assume ruolo di vigilanza dei processi interni alla struttura e la responsabilità della sicurezza dei dati
Benefici economici per circa 2,3 miliardi di € all'anno per le aziende europee (ENISA).

.

Lecito attendersi quindi un gran fermento in materia; la scarsa informazione e la difficoltà di poter ristrutturare i processi aziendali caratterizzeranno i primi mesi dell'anno. Il regolamento è ancora poco conosciuto, troppe organizzazioni continueranno ad avere un approccio cauto, senza comprendere a pieno gli obblighi ma anche i potenziali vantaggi derivanti dal regolamento. Ci aspettiamo preoccupanti ripercussioni per le imprese.
Il regolamento avrà un impatto significativo sui team di sicurezza di tutte le aziende, principalmente quelle che operano in un contesto internazionale.
Infine, uno scenario che potrebbe emergere dopo l'introduzione del regolamento vede l'applicazione della pratica estorsiva ad aziende non conformi al GDPR che una volta vittime di una violazione sono ricattate per evitare la divulgazione dell'incidente e la conseguente applicazione delle sanzioni previste. Alcune aziende potrebbero infatti esser tentate dal pagare il silenzio di gruppi criminali su un incidente che li vede protagonisti

Ransomware: una minaccia pericolosa per l'impresa

Il modello estorsivo continuerà a rappresentare una ghiotta opportunità per le organizzazioni di cyber criminali, ed i ransomware ne rappresentano la massima espressione.
L'analisi dei dati relativi agli attacchi osservati negli scorsi 12 mesi rivela uno sconcertante scenario in cui le aziende di tutto il mondo hanno subito perdite per miliardi di dollari.
Un esempio su tutti è quello relativo al caso del malware NotPetya; da sola questa minaccia ha causato svariate centinaia di milioni di dollari di perdita ad alcune multinazionali.
Secondo il rapporto economico pubblicato dal gigante dei trasporti Maersk relativo al secondo trimestre del 2017, sono stimate perdite tra 200 e 300 milioni di dollari imputabili a importanti "interruzioni del business" a causa dell'infezione causata dal ransomware.
La Reckitt Benckiser, produttrice del farmaco Nurofen e dei preservativi Durex, ha stimato un impatto sulle vendite per il secondo trimestre di circa 110 milioni di sterline. Parliamo di solo due aziende tra la moltitudine di vittime di NotPetya.
Se a questa aggiungiamo le numerose campagne malware scoperte nel 2017 (da WannaCry a Petya) e consideriamo che la maggior parte delle vittime non denuncia l'accaduto possiamo comprendere che la portata del fenomeno è significativamente maggiore.
Purtroppo il numero di famiglie di ransomware è destinato ad aumentare così come il numero di attacchi; si prevedono attacchi sempre più sofisticati ed in grado di eludere gli attuali sistemi di difesa, rivolti verso dispositivi mobili.
L'interesse in questa pratica criminale spingerà un numero crescente di attori malevoli ad implementare servizi di Ransom-as-a-Service che forniscono tutto il supporto necessario a coloro che intendono lanciare la propria campagna ransomware.
Nell'immagine seguente è riportata la tabella delle principali minacce cibernetiche; osserviamo che i malware guidano la graduatoria ed i ransomware continuano inesorabili la loro scalata.

Top Threats 2016	Assessed Trends 2016	Top Threats 2017	Assessed Trends 2017	Change in ranking
1. Malware		1. Malware		→
2. Web based attacks		2. Web based attacks		→
3. Web application attacks		3. Web application attacks		→
4. Denial of service		4. Phishing		↑
5. Botnets		5. Spam		↑
6. Phishing		6. Denial of service		↓
7. Spam		7. Ransomware		↑
8. Ransomware		8. Botnets		↓
9. Insider threat		9. Insider threat		→
10. Physical manipulation/damage/ theft/loss		10. Physical manipulation/damage/ theft/loss		→

Figure 1 Top 10 Minacce cibernetiche (ENISA Threat Landscape Report 2017)

Cybercriminali e Criptovalute

Le criptovalute possono rappresentare un bene di rifugio o sono solo oggetto di speculazione? Difficile dirlo, l'unica certezza è che l'aumento dei valori delle principali criptovalute come Bitcoin ed Ethereum continua ad attrarre l'interesse dei gruppi criminali.
Secondo il rapporto Tech Crime Trends 2017 pubblicato dall'azienda Group-IB il danno totale causato da attacchi contro sistemi di criptovalute ammonta a oltre 168 milioni di dollari e il bottino dagli attacchi ai sistemi di cambio di criptovalute varia da $ 1,5 milioni per il furto a Bitcurex fino a $ 72 milioni per l'attacco a Bitfinex. Questo dato deve indurre ad una riflessione; secondo l'azienda Group-IB, un attacco andato a buon fine contro una banca può fruttare in media solo $ 1,5 milioni, sicuramente inferiore al furto di criptovalute.
Osserveremo quindi un crescente numero di azioni contro aziende del settore con l'intento di rubare fondi attraverso attacchi di phishing o DNS hijacking.
Si osserverà un'intensificazione delle campagne di scansione della rete Internet per l'individuazione di portafogli di criptovalute accidentalmente esposti online.

Non solo furti di criptovalute, i criminali informatici sono interessati anche alle attività di mining sfruttando le risorse degli ignari utenti, ecco perché osserveremo un aumento degli attacchi basati su malware che una volta infettato un sistema ne usano la capacità computazionale per produrre criptovaluta.
Altro fenomeno in preoccupante aumento è la compromissione di siti web legittimi per l'installazione di script in grado di sfruttare le macchine dei visitatori per le attività di mining.

APT Russe e Cinesi: sempre più pericolose

Un numero crescente di governi affianca ad operazioni militari convenzionali, sofisticate campagne di cyber spionaggio e sabotaggio. A preoccupare maggiormente gli esperti di sicurezza sono gruppi APT russi e cinesi che si sono distinti nell'ultimo biennio. Il livello di complessità delle loro operazioni rende difficile l'attribuzione ed al tempo stesso espone a seri rischi qualunque organizzazione.

Organizzazioni governative, ambasciate ed aziende private continueranno ad essere i principali obiettivi di nation-state actor.

Attacchi di spear-phishing e watering hole continueranno ad essere i principali vettori utilizzati da questi gruppi; tuttavia negli scorsi mesi abbiamo assistito al preoccupante fenomeno degli attacchi alle supply chain (letteralmente la catena di approvvigionamento di un software o hardware). L'attacco NotPetya è partito con la compromissione della supply chain dell'azienda Ucraina MeDoc, discorso analogo per il caso del software CCleaner.

Il rischio è che gruppi APT (Advanced Persistent Threat) possano adottare questa tecnica per colpire obiettivi specifici riuscendo a restare nascosti per periodi molto lunghi.

Sicurezza del Cloud: una priorità assoluta per le imprese

Nel 2018 un numero crescente di aziende utilizzerà servizi in cloud, spesso senza avere alcuna consapevolezza dei rischi cui sono esposti.
Secondo Forbes, nei prossimi 15 mesi, l'80% del budget IT delle aziende sarà destinato all'adozione di soluzioni in cloud, tuttavia circa il 49% delle aziende sta ritardando il passaggio al cloud a causa di un'importante mancanza di competenze in tema di cyber security.
Le infrastrutture cloud rappresentano un bersaglio privilegiato per differenti categorie di attaccanti e purtroppo poche sono le aziende che adotteranno una strategia di sicurezza efficace che consenta di mitigare il rischio di esposizione alle minacce cibernetiche.

Dispositivi IoT: un obiettivo privilegiato degli hacker

Il numero di attacchi informatici contro i dispositivi dell'Internet delle Cose è destinato ad aumentare in maniera significativa e con esso il numero degli attacchi nei confronti di questa famiglia di dispositivi.
La mancata implementazione di requisiti minimi di sicurezza e configurazioni errate saranno le principali ragioni del successo degli attacchi contro questa categoria di dispositivi.
Gli attacchi sono principalmente condotti per compromettere sistemi dell'Internet delle cose e reclutarli in botnet composte da decine se non centinaia di migliaia di sistemi. Una botnet di dispositivi IoT può essere utilizzata per scopi molteplici, come un attacco di DDoS.

Secondo un rapporto pubblicato in novembre dall'azienda di sicurezza Corero, il numero di attacchi di DDoS è raddoppiato nella prima metà del 2017 proprio a causa del coinvolgimento di dispositivi non protetti dell'Internet delle Cose.
Alcuni sistemi potrebbero essere particolarmente esposti, come ad esempio dispositivi basati su ARC-CPU, che per la prima volta sono stati oggetto di un attacco di un malware appositamente concepito chiamato Mirai Okiru. Considerando che ogni anno sono prodotti circa 1,5 miliardi di dispositivi basati su ARC-CPU, possiamo comprendere il potenziale impatto di una simile infezione.
Fortunatamente, i produttori di dispositivi dell'Internet delle cose dedicheranno maggiore attenzione agli aspetti di sicurezza dei loro dispositivi rendendo più difficile la loro compromissione.
Possibile che si vada verso la definizione di un quadro normativo che obblighi all'adozione di misure minime di sicurezza.

Dispositivi Mobili sotto assedio

Nel 2018, il numero di minacce per dispositivi mobili continuerà a crescere ed il sistema operativo mobile Google Android sarà il principale bersaglio di criminali informatici.
Continuerà il trend osservato nel corso del 2017 relativo alla diffusione di mobile malware attraverso false applicazioni pubblicate nello store ufficiale di Google, il Play Store.
Banking Trojan e ransomware mobile saranno le principali minacce ai sistemi mobili.
Nell'underground criminale aumenterà in modo significativo l'offerta specifica per quanto concerne minacce ai sistemi mobili, codici malevoli e servizi di Malware-as-a-Service saranno facilmente reperibili nei principali blackmarket, in particolare nell'ecosistema criminale cinese.
Sia Google che Apple perfezioneranno i loro sistemi per l'identificazione delle applicazioni potenzialmente dannose pubblicate nei loro store.

Conclusioni

É sempre più urgente predisporre nuove norme di comportamento, anche a livello istituzionale e transnazionale, com'è stato ribadito a più riprese, anche in sede di *G7*, ma mentre la sensibilità delle istituzioni aumenta, è necessario organizzarsi con urgenza, assumendo iniziative efficaci per proteggersi – e proteggere i propri stakeholder – dai rischi di un attacco cyber.
In CybSec, ripetiamo spesso che la cyber security ha un ineludibile aspetto tecnologico, ma non si esaurisce in esso: chi decide di agire per proteggere i propri sistemi digitali, protegge i propri asset patrimoniali più strategici.
L'accesso alle tecnologie più sofisticate presenti sul mercato internazionale dev'essere integrato efficacemente nel proprio specifico sistema di procedure aziendali: è necessario verificare l'architettura dei flussi interni e dei livelli di accesso alle informazioni critiche, effettuare training del personale, immaginare protezioni assicurative e legali per la mitigazione del rischio, e concludere accordi per disporre di assistenza immediata in caso di attacchi e di crisi.
Tutti sono potenziali obiettivi, e questo sarà ancor più vero, con l'avverarsi degli scenari sopra descritti, nel corso del 2018.

Per un contatto immediato con il nostro team:
www.csecybsec.com
email: info@csecybsec.com
+39 06 85352121

CSE Cybsec SPA
www.csecybsec.com
info@csecybsec.com