kaspersky

Policy Newsletter

Secondo semestre 2020

Alla fine dell'anno spesso si tirano le somme guardando a quello che è stato e a quello che sarà. La pandemia di Covid-19 costituisce una grande sfida da gestire che ha colpito ogni settore dello stato, della società e dell'economia. La pandemia ha messo a nudo le debolezze e la necessità di agire.

Ha inoltre evidenziato come sia importante una **digitalizzazione sicura e affidabile**. Tutti i player si sono trovati di fronte a questa sfida. L'Unione Europea e i suoi Stati membri hanno dovuto prendere molte decisioni difficili, dovendo gestire nel contempo le attività quotidiane. Per quanto riguarda in particolare la cyber sicurezza è importante stare al passo, definire la giusta linea d'azione fin da subito e consolidare in modo sostenibile la cooperazione e lo scambio di informazioni di questa sfida **transfrontaliera**. Come azienda globale di cybersecurity il nostro impegno è rivolto in questa direzione: il nostro obiettivo è accrescere la resilienza del cyberspazio nel lungo termine, negli Stati membri, in Europa e su scala globale.

Per questo motivo abbiamo ampliato ulteriormente la nostra Global Transparency Initiative, definito un Cyber Capacity Building Program e, seguendo il concetto di **cyber-immunità**, ci stiamo focalizzando su un chiaro approccio di **security-by-design**. Con questa newsletter vogliamo offrire impulsi e idee e delineare possibili strategie e incentivare uno scambio di opinioni e esperienze.

Morten Lehn
General Manager Italy,
Kaspersky

Sicurezza e integrità della supply chain digitale: prosegue la Global Transparency Initiative

Lanciata nel 2017, la Global Transparency Initiative (GTI) di Kaspersky ha l'obiettivo di mostrare al mondo che la nostra azienda non ha nulla da nascondere, e che i nostri clienti possono fidarsi di noi. Non ci limitiamo a chiedere fiducia ma siamo pronti a dimostrare che la meritiamo. Dopo i successi conseguiti negli ultimi anni, tra cui la certificazione ISO27001 che conferma la validità dei sistemi di sicurezza dei dati dell'azienda, a novembre abbiamo avuto il piacere di annunciare gli ultimi sviluppi della GTI:

È stato completato il trasferimento in Svizzera dei dati della Kaspersky Security Network.

Oltre a Europa, USA e Canada, Kaspersky ha trasferito l'archiviazione e l'elaborazione dei dati degli utenti in Australia, Nuova Zelanda, Giappone, Bangladesh, Brunei, Cambogia, India, Indonesia, Sud Corea, Laos, Malesia, Nepal, Pakistan, Filippine, Singapore, Sri Lanka, Tailandia e Vietnam. I dati sulle minacce condivisi dagli utenti in questi Paesi ora vengono elaborati presso due data center con sede a Zurigo, in Svizzera. Questi dati includono file malevoli sospetti o precedentemente sconosciuti che vengono inviati dai prodotti dell'azienda alla rete Kaspersky Security Network (KSN) per l'analisi automatizzata dei malware. automated malware analysis.

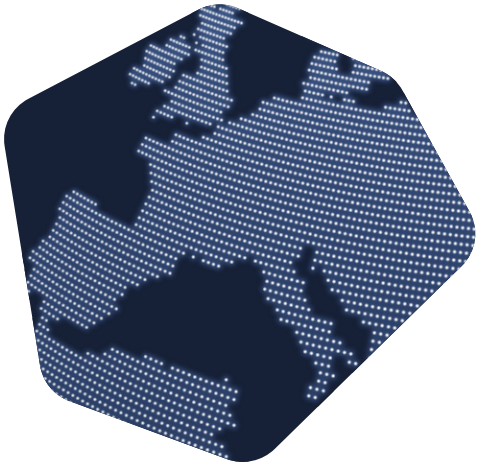
Attualmente sono operativi quattro centri di trasparenza per la revisione del codice sorgente

in Svizzera, Spagna, Malesia e Brasile. Viene offerta inoltre la possibilità ai nostri partner di accedere da remoto per conoscere i metodi di engineering e gestione dati di Kaspersky. Il prossimo passo sarà l'apertura di un Transparency Center in Canada che sarà operativo a partire dall'inizio del 2021 in partnership con l'organizzazione no profit CyberNB.

È stato lanciato il Cyber Capacity Building Program sulla valutazione della sicurezza del prodotto per i governi:

la prima fase del programma è stata realizzata con un'agenzia di cyber sicurezza nazionale del Sud-est asiatico, seguita da una sessione dedicata agli accademici europei e africani nel dicembre 2020. Ora siamo pronti ad offrire questa formazione dedicata alla revisione del software alle organizzazioni private per migliorare la loro resilienza contro i rischi della supply chain.

L'obiettivo di questi aggiornamenti è fare in modo che la trasformazione digitale garantisca la sicurezza e l'integrità della supply chain. È possibile avere maggiori informazioni e richiedere l'accesso ai nostri Transparency Center accedendo a questo link.



Revisione Direttiva NIS: un'opportunità per un mercato unico digitale armonizzato nella UE

La Commissione Europea intende sottoporre, entro metà dicembre, la sua proposta di revisione della Direttiva sulla sicurezza della rete e dei sistemi informatici all'interno dell'Unione (Direttiva NIS). Tale direttiva, entrata in vigore nel 2016 come primo atto legale sulla cyber sicurezza della UE, fa parte della politica e della strategia di cybersecurity della UE. Nel 2020, la Commissione Europea ha annunciato la revisione della Direttiva NIS allo scopo di potenziare la cyber sicurezza e ha lanciato una consultazione pubblica per contribuire alla sua revisione.

Il contributo di Kaspersky

Poiché la revisione della direttiva NIS è prossima e sarà una pietra miliare dell'agenda europea per i prossimi mesi, Kaspersky non si è fatta attendere per offrire il suo contributo a questo dibattito.

Webcast dell'Unione Europea sulla revisione della Direttiva NIS

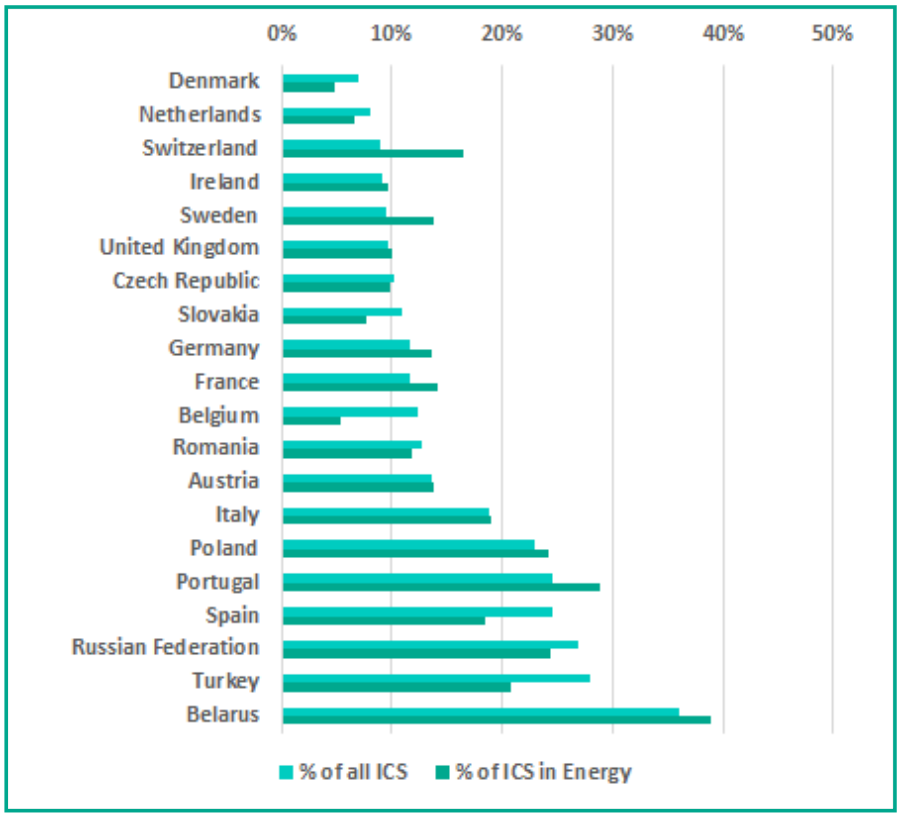
Il 9 settembre 2020, Kaspersky ha organizzato un secondo Cybersecurity Webcast europeo che aveva come titolo "Review of the NIS Directive – from cybersecurity to cyber-immunity?". Forte del successo del precedente (e primo) webcast di Kaspersky tenuto a luglio 2020 ("Technology that works for people: Why the right level of cybersecurity is crucial for digitalization"), il forum ha riunito oltre 150 partecipanti europei e ha visto la partecipazione di relatori di prim'ordine provenienti da diversi gruppi di stakeholder e regioni che hanno discusso sulle opportunità legate alla revisione della Direttiva NIS. Tra i relatori: Evangelos Ouzounis, Head of Secure Infrastructure and Services at ENISA; il CEO di Kaspersky Eugene Kaspersky; Susanne Dehmel, Member of the Executive Board, Legal & Security at Bitkom; e Corrado Giustozzi, membro di CERT-AGID Italia, esperto di cyber sicurezza e docente all'università 'La Sapienza' di Roma. È possibile vedere la registrazione qui.

Kaspersky ha presentato il suo contributo sia alla valutazione della roadmap che a quella dell'analisi di impatto iniziale (inception impact assessment) sulla direttiva NIS ed anche in occasione della consultazione pubblica sulla revisione della direttiva stessa. Kaspersky sprona il massimo organo direttivo della UE a proseguire il percorso di armonizzazione del mercato unico digitale europeo e a promuovere un più coerente campo d'azione comune sia per gli operatori di servizi essenziali (OSE) che per i fornitori di servizi digitali (FSD) all'interno della UE. A nostro avviso, l'attuale frammentazione – che è il risultato di diverse legislazioni, delle diverse applicazioni della direttiva e delle numerose definizioni proprie degli Stati membri - può essere superata con una direttiva che potrebbe servire da modello per altre regioni e contribuire all'armonizzazione e standardizzazione globale nell'ambito della sicurezza delle reti e dei sistemi informatici.

Sebbene Kaspersky riconosca come la direttiva NIS abbia sostenuto e ulteriormente accelerato lo sviluppo delle risorse di cybersecurity all'interno degli Stati membri UE, si assiste però a scenari di minacce in costante evoluzione che minacciano le reti e i sistemi informatici. A questo proposito, si può solo chiedere alla Commissione di introdurre delle modifiche mirate all'attuale direttiva, nell'ottica di chiarire alcune disposizioni e armonizzare ulteriormente le normative vigenti. Tra gli aspetti che necessitano di revisione, riteniamo che, dal momento che la Direttiva NIS costituisce il più importante atto legislativo di contrasto alle minacce rivolte alla sicurezza informatica, integrare la direttiva European Critical Infrastructure (ECI) del 2008 nella direttiva NIS rivista contribuirebbe notevolmente all'armonizzazione del mercato unico digitale europeo, in quanto eviterebbe di duplicare la legislazione, sarebbe coerente con la nostra volontà di ridurre la frammentazione, e sarebbe in linea con la valutazione della Commissione 2009 della direttiva ICE, che chiedeva un "ulteriore allineamento" con la direttiva NIS.

Dati e cifre

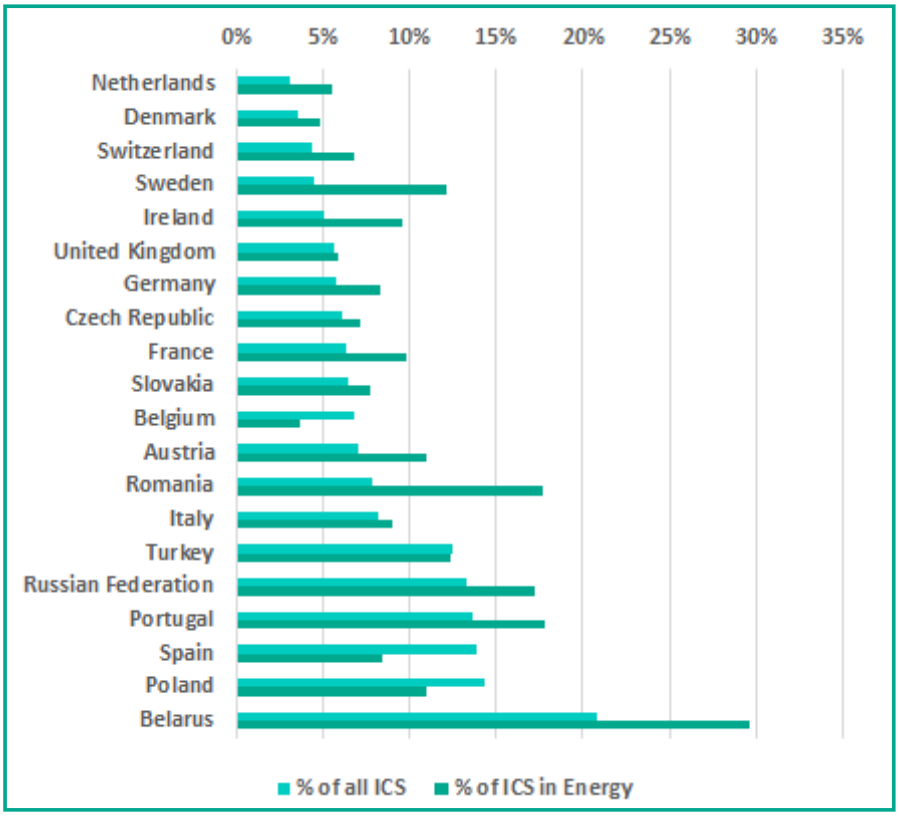
Gli esempi più sorprendenti della necessità di proseguire nell'impegno di creare funzioni di cyber sicurezza più resilienti in Europa, in particolare nel settore energetico, si possono cogliere guardando l'ultima ricerca ICS CERT di Kaspersky sulle cyber minacce per i sistemi di controllo industriale (ICS) nel settore energetico in Europa.



Confrontando la percentuale di tutti i computer ICS sui quali è stato bloccato un malware con la stessa percentuale dei computer ICS in uso nel settore energetico nel primo trimestre 2020, si osserva che in molti paesi (Svizzera, Svezia, Francia, Germania, Polonia, Portogallo e Bielorussia) la percentuale di computer ICS nel settore energetico sui quali è stato bloccato un malware è stata molto più elevata rispetto alla corrispondente percentuale per tutti i computer ICS utilizzati in quei Paesi.

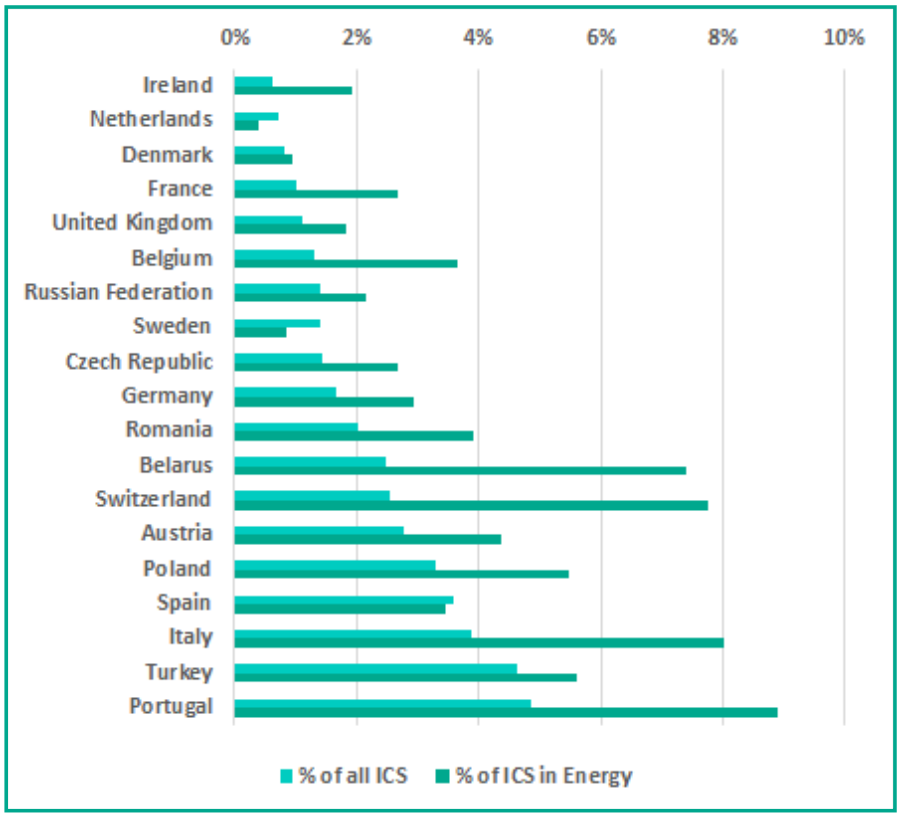
Percentuale di computer ICS sui quali è stato bloccato un malware: comparazione tra tutti i computer ICS e i computer ICS nel settore energia, Europa, 1° trimestre 2020

Questo divario tra gli Stati europei è ancora più evidente se si confronta la percentuale di tutti i computer ICS su cui sono state bloccate minacce provenienti da internet nei Paesi europei con una percentuale simile per i computer ICS utilizzati nel settore energia nel primo trimestre 2020. In questo caso, solo quattro Paesi (Belgio, Turchia, Spagna e Polonia) riscontrano un numero inferiore di minacce nel settore energetico rispetto agli altri.

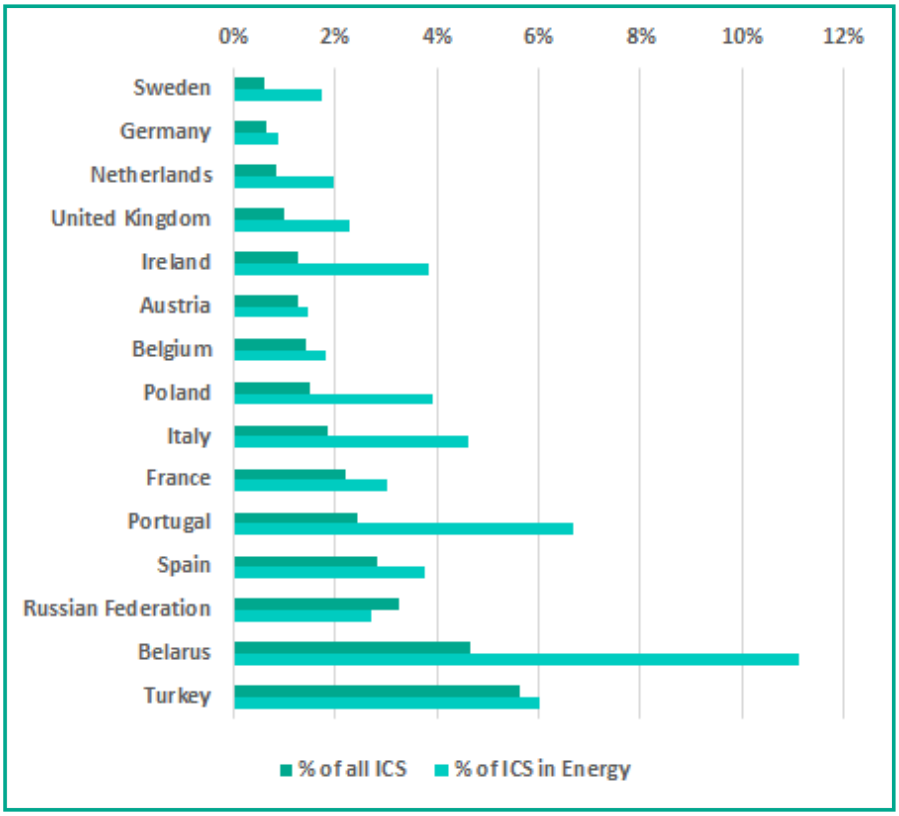


Percentuale di computer ICS su cui sono state bloccate minacce provenienti da Internet: comparazione tra tutti i computer ICS e i computer ICS nel settore energia, Europa, 1° trimestre 2020.

Lo stesso trend si osserva anche quando si guarda alle minacce via e-mail o da supporti remobivili: le organizzazioni nei Paesi in cui i computer ICS nel settore energetico bloccano più attivamente le cyber minacce dovrebbero adottare misure aggiuntive per proteggere i loro sistemi informatici dagli attacchi.



Percentuale di computer ICS su cui sono state bloccate minacce vie e-mail: comparazione tra tutti i computer ICS e i computer ICS nel settore energia, Europa, 1° trimestre 2020.



Percentuale di computer ICS su cui sono state bloccate minacce da supporti removibili: comparazione tra tutti i computer ICS e computer ICS nel settore energia, Europa, 1° trimestre 2020.

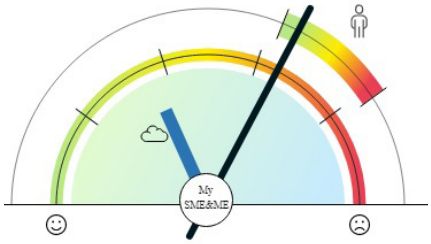
Per saperne di più: https://ics-cert.kaspersky.com/

Kaspersky supporta Horizon 2020 il programma promosso dalla Commissione Europea per il finanziamento di progetti di Ricerca e Innovazione

Nell'ambito di **HORIZON 2020, il programma promosso dalla Commissione Europea per il finanziamento di progetti di Ricerca e Innovazione**, nascono tre progetti di innovazione nei quali Kaspersky è stato coinvolto grazie alla sua expertise nel campo della cybersecurity.

A giugno è stato lanciato **GEIGER**, un progetto di innovazione ideato da un consorzio di 18 organizzazioni che ha l'obiettivo di sviluppare una soluzione che sia in grado non solo di dimostrare alle piccole imprese e agli imprenditori quali sono i rischi di sicurezza informatica per la loro azienda legati alla protezione dei dati e alla privacy ma anche di offrire assistenza per ridurre questi rischi al minimo.

Al progetto collaboreranno specialisti ed esperti di cybersecurity e centri nazionali di sicurezza informatica per sviluppare Cyber-GEIGER, un "rilevatore Geiger" per la sicurezza informatica, che aiuterà le piccole imprese a prendere coscienza dei rischi ai quali sono esposte. Le piccole imprese potranno utilizzare Cyber-GEIGER dal web o dallo smartphone e ottenere tutte le informazioni sul livello di rischio attuale della propria azienda. Prendere coscienza dei rischi permette all'utente di poter rispondere in maniera efficace attraverso l'adozione di semplici misure o la richiesta di assistenza per ridurre significativamente l'esposizione al rischio.



A settembre, Kaspersky ha presentato il secondo progetto previsto dalla Commissione europea in tema di innovazione. Si tratta di **CitySCAPE** che ha lo scopo di proteggere l'ecosistema dei trasporti multimodali. Il progetto coinvolge **15 partner da 6 diversi Paesi europei**, uniti dall'obiettivo comune di soddisfare le esigenze di sicurezza informatica del trasporto multimodale. CitySCAPE introduce tecniche innovative di analisi del rischio e gestisce una serie di soluzioni software per realizzare un toolkit interoperabile che si integri perfettamente in qualsiasi sistema di trasporto multimodale. La soluzione CitySCAPE sarà testata in due casi d'uso e nel test saranno coinvolte applicazioni di ticketing, sistemi automatici di controllo e moduli di gestione di veicoli connessi e a guida autonoma, al fine di dimostrarne l'efficacia. I due progetti pilota in CitySCAPE verranno realizzati nel sistema di trasporto locale di Genova, in Italia e di Tallinn, in Estonia.

A novembre è stato lanciato anche il terzo progetto Horizon 2020, **TRAPEZE** che si pone l'ambizioso obiettivo di guidare il cambiamento culturale nella protezione dell'economia europea dei dati ed è finalizzato allo sviluppo di una soluzione che consenta di mettere nelle mani dei cittadini UE la sicurezza e la privacy dei propri dati. Il progetto aprirà la strada all'utilizzo pratico delle tecnologie d'avanguardia a favore dei cittadini.

Grazie alla sua expertise nel campo della cybersecurity, **Kaspersky** è stata coinvolta nello sviluppo dei tre progetti ed è parte dei tre consorzi. L'azienda metterà a disposizione le proprie soluzioni e i servizi di sicurezza innovativi. In particolare, Kaspersky è responsabile della protezione delle applicazioni mobile attraverso l'integrazione con il Kaspersky Mobile Security Software Development Kit (KMS SDK), una soluzione che offre protezione per i dispositivi mobili contro minacce note ed emergenti. Si tratta di un framework multilivello che offre una protezione online integrata direttamente nelle applicazioni mobili, proteggendo in tempo reale le informazioni inserite dagli utenti e le transazioni su dispositivi mobile con sistemi operativi Android, iOS e Windows Phone. Inoltre, Kaspersky si occuperà della formazione degli utenti attraverso le soluzioni di gamification "Cyber Safety Management Games (CSMG)" e "Kaspersky Interactive Protection Simulation (KIPS)" e attraverso la soluzione di training online "Kaspersky Automated Security Awareness Platform (K-ASAP)". Si tratta di un programma di formazione che, attraverso il micro-apprendimento e la competizione, favorisce l'impegno delle imprese e degli utenti finali verso la cybersecurity. La formazione offerta da Kaspersky fornisce competenze, conoscenze e comportamenti essenziali per mantenere un ambiente di lavoro sicuro e proteggere la propria privacy. Copre tutti i principali ambiti di sicurezza e le situazioni tipiche. Inoltre, dove previsto, Kaspersky alimenterà le piattaforme di Threat Intelligence con i suoi Threat Data Feeds al fine di contribuire ad anticipare gli incidenti causati da minacce APT (Advanced Persistent Threats).

> "Siamo davvero molto orgogliosi di partecipare a questi tre progetti e di poter contribuire alle soluzioni per cittadini, piccole imprese e utenti dei sistemi di trasporto multimodali con i nostri prodotti e servizi professionali nel campo della cyber security", **ha dichiarato Amedeo D'Arcangelo, Enterprise Project Technical Coordinator di Kaspersky.** "Nei consorzi di cui facciamo parte siamo considerati un partner affidabile sia per merito delle nostre competenze tecniche, che ci consentono di proteggere e formare aziende e utenti in ogni settore, che per la nostra cultura dell'innovazione, che ci permette di adattare prodotti e servizi e di crearne di nuovi in un contesto in continua evoluzione quale quello delle minacce alla sicurezza informatica".

Cosa abbiamo imparato dal 2020 e cosa dobbiamo aspettarci dal 2021

Giampaolo Dedola, ricercatore sicurezza senior del Global Research and Analysis Team (GReAT) di Kaspersky fa un'analisi di quanto accaduto nel 2020 e ci racconta quali saranno le minacce che ci aspettano nel 2021.

Quali sono le minacce che si sono evolute nel 2020 e che probabilmente vedremo svilupparsi ulteriormente anche nel 2021 ?

La pandemia ha indubbiamente modificato il nostro stile di vita. Il trasferimento improvviso di milioni di dipendenti dai propri uffici alle abitazioni ha imposto alle aziende di dotarsi velocemente di sistemi che permettessero il lavoro da remoto. Inoltre, le misure di distanziamento sociale hanno spostato sul web molte altre attività della vita quotidiana, come lo studio, gli acquisti e l'entertainment. Questo ha contribuito ad un aumento delle superfici di attacco e ha facilitato l'attività degli attaccanti. Siamo certi che le infrastrutture messe in piedi dalle aziende nel 2020, come VPN o server RDP, non verranno dismesse ma continueranno ad essere sfruttate anche il prossimo anno per consentire ai dipendenti di continuare a svolgere, in parte, il loro lavoro da remoto. È logico quindi pensare che anche gli attaccanti continueranno a sfruttarle per penetrare all'interno delle infrastrutture aziendali. Abbiamo anche osservato come il numero crescente di dispositivi network e di utenti che ne richiedevano l'accesso abbia contribuito ad aumentare l'esposizione delle aziende rendendo più semplice ai criminali informatici il furto di credenziali valide per accedere e penetrare all'interno del perimetro aziendale. La pandemia non è stata l'unica protagonista delle minacce del 2020. Abbiamo anche osservato l'evolversi di alcuni attacchi come ad esempio i ransomware mirati, un fenomeno che ha avuto inizio nel 2018 e che ha continuato a svilupparsi anche nel 2020. È aumentato il numero di attacchi di questo tipo soprattutto nei confronti di aziende di medie e grandi dimensioni in Europa e in Nord America. Questi attacchi oltre a raggiungere livelli altissimi di sofisticazione hanno utilizzato un nuovo sistema per raggiungere i propri obiettivi, ovvero la doppia estorsione. Inizialmente i ransomware si limitavano a bloccare l'accesso ai file dell'utente con l'obiettivo di richiedere un riscatto in cambio dello sblocco. Nel 2020 abbiamo osservato l'aggiunta di un elemento in più nella richiesta di riscatto. Adesso gli stessi attaccanti una volta preso il controllo della rete aziendale, oltre a bloccare l'accesso ai file, rubano i dati sensibili per poi minacciare le aziende di diffonderli pubblicamente. Questa evoluzione siamo sicuri che continuerà anche nel 2021 in quanto gli attaccanti sono riusciti ad accumulare una quantità enorme di risorse economiche che gli consentirà di migliorare i propri toolkit.

Cosa bisogna fare per difendersi?

La strategia più adeguata a proteggersi da minacce sempre più sofisticate è sicuramente quella di adottare un approccio multilivello. Questo vuol dire che non è più possibile affidarsi ad un singolo prodotto ma è necessario che la difesa includa anche la sensibilizzazione dell'utente sulle principali problematiche di sicurezza e la maggiore visibilità e protezione sui singoli endpoint. Per fare ciò sono necessarie soluzioni personalizzate ed evolute che siano in grado identificare le minacce note ma anche quelle ancora sconosciute come nuovi malware o exploit zero-day. Ovviamente poi è necessaria anche una protezione a livello network che consenta di avere visibilità completa su ciò che accade nelle reti aziendali e identificare quelle che sono le componenti anomale e dannose. In questo caso sono fondamentali le tecnologie che sfruttano la threat intelligence e che sono quindi in grado di individuare e analizzare le minacce informatiche rivolte a un'azienda setacciando un'enorme quantità di dati al fine di riconoscere i problemi reali e mettere in atto soluzioni specifiche per il problema riscontrato. Un'altra componente fondamentale della strategia di protezione è la formazione dei dipendenti perché per raggiungere le reti aziendali gli attaccanti sfruttano con sempre maggiore frequenza la scarsa conoscenza degli utenti in materia di sicurezza informatica. Infatti, spesso l'accesso alle reti avviene attraverso attacchi molto semplici che mirano ad ingannare l'utente. Come ad esempio il phishing o le minacce che invitano l'utente ad aprire risorse malevole inviate tramite email standard. Per mitigare questo problema esistono corsi di formazione in grado di garantire all'utente l'acquisizione di tutte le informazioni necessarie ad identificare comportamenti e oggetti anomali consentendo una riduzione sostanziale dell'esposizione dell'azienda. Infine, ci troviamo spesso ad osservare come sia ancora troppo frequente la mancanza di una visione di insieme delle informazioni presenti nell'infrastruttura aziendale. Le aziende, infatti, spesso non hanno idea di quali siano le informazioni esposte o gli asset raggiungibili dall'esterno. In questo caso può essere molto utile utilizzare soluzioni che aiutino a mantenere visibilità su tutti quelli che sono i sistemi esposti e che potrebbero presentare delle criticità di sicurezza. Infine, ci teniamo a consigliare alle aziende

di non sottovalutare neppure le minacce considerate generiche come ad esempio i Trojan che possono nascondersi in email massive (vedi finte email che sfruttano il nome dell'Inps per essere più credibili) poiché il 2020 ci ha anche dimostrato come questo genere di minaccia spesso nasconda attacchi più pericolosi. Tenendo conto di questo ci auguriamo che le aziende acquisiscano maggiore consapevolezza e non si limitino più soltanto a cancellare i malware ma comincino ad effettuare attività di investigazione e di incident response anche sulle minacce meno critiche perché è molto probabile che portino ad attacchi più pericolosi.

Previsioni sulle minacce per il 2021. Attenzione a privacy, estorsioni e vaccini.

A causa della pandemia di COVID-19 il settore sanitario e la tecnologia sono stati protagonisti indiscussi del 2020. Il notevole aumento del livello di criticità delle infrastrutture mediche, unita all'aumento di una digitalizzazione trasversale, hanno contribuito a rendere il settore sanitario ancora più vulnerabile. L'utilizzo di tematiche che riguardano il settore sanitario come esca continuerà anche il prossimo anno e rimarrà rilevante almeno fino alla fine della pandemia. Il motivo principale del crescente interesse degli attaccanti per la ricerca medica è stato lo sviluppo di un vaccino contro il COVID-19. Nel 2021, l'impegno dei criminali per rubare i dati relativi alla ricerca sul coronavirus continuerà. Finché le organizzazioni sanitarie cercheranno di combattere il virus, qualsiasi azienda che rivendichi un successo significativo nello sviluppo di un vaccino diventerà una potenziale vittima di attacchi mirati. Anche il furto di cartelle cliniche diventerà parte integrante degli attacchi mirati, poiché la condivisione di informazioni accurate sui pazienti renderà i messaggi falsi molto più credibili. Tuttavia, l'attenzione alla sicurezza digitale negli ospedali offre la speranza che nel 2021 ci possa essere una maggiore collaborazione tra esperti di sicurezza e organizzazioni e sistemi sanitari. L'esperienza ha dimostrato che le grandi crisi, come lo è stata questa pandemia, spingono le organizzazioni a prestare maggiore attenzione alla protezione delle loro infrastrutture.

Il 2020 è stato anche l'anno in cui il settore dell'istruzione ha subito una svolta decisiva: 1,5 miliardi di studenti hanno dovuto seguire le lezioni a distanza con educatori costretti a districarsi nel tentativo di padroneggiare nuovi strumenti e, al contempo, mantenere un livello di istruzione alto. Il processo di digitalizzazione del settore dell'istruzione a cui abbiamo assistito nel 2020 è destinato a continuare anche nel 2021. Da un lato trarremo enormi benefici dalla possibilità di sfruttare nuovi strumenti e opportunità, compresi quelli che in origine non erano affatto collegati all'istruzione, come ad esempio TikTok. Inizialmente, infatti, gli insegnanti preferivano YouTube, ma nel 2020 TikTok è diventato una piattaforma popolare per la produzione di contenuti educativi. Dall'altro lato però l'utilizzo di nuovi strumenti digitali comporterà anche la nascita di nuove minacce. La preoccupazione maggiore in questo caso riguarda la privacy. Le piattaforme di e-learning solitamente delegano l'utente per l'impostazione delle regole per la privacy, ma molti di loro (soprattutto i bambini più piccoli) non sanno come controllare in modo appropriato queste impostazioni. Inoltre, la varietà di servizi che forniscono strumenti educativi online può complicare ulteriormente le cose. Sarà quindi necessario prestare attenzione, ad ogni tool e ad ogni situazione e proteggere non solo le proprie informazioni personali ma anche quelle degli studenti.

Infine, non possiamo non guardare al settore industriale. Nel 2020 alcuni gruppi criminali hanno esaminato attentamente le caratteristiche delle organizzazioni industriali ottenendo l'accesso a grandi quantità di informazioni sulle loro reti. Questo trend dovrebbe continuare anche nel 2021. In particolare, gli attacchi ransomware contro i sistemi ICS diventeranno più mirati e, di conseguenza, ancora più sofisticati grazie alle tattiche APT. Si tratta di una minaccia significativa, poiché le reti industriali sono diventate più vulnerabili a causa dei limiti imposti sulla presenza dei dipendenti sul luogo di lavoro, unitamente all'aumento del numero di persone che accedono alle reti da remoto.

Affrontare i problemi informatici a IGF 2020

A novembre, Kaspersky ha avuto la possibilità di partecipare ad Internet Governance Forum (IGF 2020), piattaforma multi stakeholder globale che facilita la discussione dei problemi politici pubblici legati ad Internet.

In occasione della sessione online dedicata alla situazione della cyber sicurezza in tempi di Covid (High-Level Leaders Track: Security'), il CEO Eugene Kaspersky ha espresso il suo pensiero su come l'attuale pandemia abbia cambiato la politica dell'equilibrio tra gli hacker e le potenziali vittime. A suo parere, la situazione ai tempi del Covid è chiaramente più pericolosa di prima, in particolare per due fattori:

"Il primo fattore è che oggi molte persone stanno a casa, dunque passano più tempo su Internet e i malintenzionati possono facilmente colpire più vittime di prima. Il secondo fattore è che molte aziende fanno stare a casa i propri dipendenti. Le persone lavorano da casa con un livello di sicurezza di base, anche se possono accedere alla rete aziendale, e dunque i criminali violano i computer domestici e accedono così alle reti aziendali."

Come esempio concreto della crescita dei cyber attacchi, Eugene Kaspersky ha analizzato il forte aumento di nuove applicazioni malevole durante la pandemia Covid rispetto al periodo pre-pandemia:

"Prima del Covid, registravamo circa 350.000 nuove applicazioni malevole al giorno. In questo momento raccogliamo più di 400.000 file malevoli al giorno, il che significa che il cybercrime globale è ancora più attivo"

Il moltiplicarsi delle minacce non è però il solo elemento a preoccupare. Un altro grande problema che contribuisce a deteriorare la situazione del mondo informatico è la grande professionalità degli hacker e come la pandemia consenta loro di ripensare e affinare i loro metodi, fino a formare le cosiddette "gang criminali". Considerando quest'ultimo sviluppo, c'è da temere che gli attacchi dei cyber criminali saranno sempre più mirati alle infrastrutture in generale, ma anche alle infrastrutture fisiche. Nelle parole di Eugene Kaspersky:

"Il problema crescente è che molti di questi giovani cyber criminali sono sempre più bravi ed esperti e si stanno alleando ai team di hacker professionali. (...) Temo che il prossimo passo saranno degli attacchi massicci alle infrastrutture e alle infrastrutture fisiche"

Poiché non è possibile sviluppare soluzioni di cybersecurity singolarmente per ogni dispositivo o oggetto connesso (p.e. fotocopiatrici, aspirapolvere, telecamere di sicurezza), Eugene Kaspersky ha infine suggerito la necessità di creare sistemi che siano sicuri by design e ha promosso il concetto di 'cyber-immunità' di Kaspersky.

Prima di questo evento di alto livello, Kaspersky ha anche organizzato (o presenziato) altri workshop su un'ampia varietà di temi legati alla cyber sicurezza. I link alle registrazioni di queste sessioni si possono trovare qui:

- Stop stalkerware: tackling digital stalking helps victims of domestic violence – (Stop agli stalkerware: affrontare lo stalking digitale aiuta le vittime di violenze domestiche), organizzata insieme alla Coalizione contro gli stalkerware
- Security of digital products: Industry and enhancing trust - (Sicurezza dei prodotti digitali: industria e accrescere la fiducia)
- Assurance and transparency in ICT supply chain security – (Assicurazione e trasparenza nella sicurezza della supply chain ICT), organizzata dall' East-West Institute e AUSIM Marocco
- Best Practice Forum on Cybersecurity - What Cybersecurity Policymaking Can Learn from Normative Principles in Global Governance-Forum (best practice sulla cybersecurity: cosa può apprendere la policy making sulla cybersecurity dai principi normativi nella governance globale)

Per finire, Kaspersky ha anche allestito uno stand presso l'IGF Village 2020 sul tema delle best practice multistakeholder avente come tema la fiducia e la responsabilità nel cyberspazio. Con questo stand l'azienda ha colto l'opportunità di presentare alcune iniziative di successo tese a migliorare il cyberspazio, ed in particolare la Global Transparency Initiative (GTI), l'iniziativa 'No More Ransom' e la Coalition Against Stalkerware.