ASA | SVV

«Più un’azienda è digitalizzata, più viene presa di mira»

Intervista | 22 Settembre 2021

La criminalità su internet ha registrato un netto aumento. Nel frattempo, più dell’80 percento degli attacchi alle aziende e ai privati è compiuto da bande criminali. Florian Schütz, delegato federale alla cibersicurezza, spiega in un’intervista chi è particolarmente esposto e come ci si può proteggere dagli attacchi anche in telelavoro.

Florian Schütz, su incarico della Confederazione, da due anni lei si occupa dei rischi informatici. Quali riflessioni e conclusioni ne trae?

Negli ultimi anni, siamo stati in grado di sensibilizzare la popolazione e le aziende sul tema della sicurezza informatica. Tuttavia, constatiamo tuttora molte differenze nella cibersicurezza, specialmente tra le aziende. Da un lato ci sono coloro che non hanno una buona preparazione e ritengono che la cibersicurezza per loro non sia fondamentale. Dall’altro, ci sono aziende che prendono l’argomento sul serio e investono in questo settore. Se si guarda alla Svizzera nel suo complesso, in termini di sicurezza informatica siamo nel mezzo. Quindi c’è ancora molto lavoro da fare.

Per quale ragione?

In particolare in economia, l’informatica è ancora percepita troppo come puro supporto: quale ausilio per la contabilità finanziaria o per la comunicazione. Eppure, l’informatica è un’importante pietra miliare per qualsiasi azienda. Pertanto, gli ingegneri informatici dovrebbero essere rappresentati ad esempio anche nella direzione per potervi introdurre argomenti come la cibersicurezza. Questo è il caso, già da molto tempo, delle aziende tecnologiche internazionali.

> «Se ai criminali basta individuare un unico punto debole per penetrare il sistema, agli ingegneri non può sfuggire neanche un errore.»

Lei stesso ha lavorato per aziende come RUAG e Zalando e ha più di dieci anni di esperienza nella sicurezza informatica. Quali sviluppi figurano in primo piano riguardo a questo argomento?

Una sfida importante è quella di sviluppare sistemi informatici che siano il più possibile invulnerabili. Vede, è una battaglia impari: se ai criminali basta individuare un unico punto debole per penetrare il sistema, agli ingegneri non può sfuggire neanche un errore.

Consiglia chiaramente di non pagare riscatti ai criminali informatici: Florian Schütz, delegato federale alla cibersicurezza. (© Keystone-SDA, Gaëtane Bally)

Quali sono le aziende o i settori particolarmente esposti?

Non parlerei di aziende o settori, ma di grado di digitalizzazione. Più un’azienda è digitalizzata, più viene presa di mira dai criminali cibernetici e maggiore è il danno che possono arrecarle rubando, ad esempio, dati personali.

Dopo tali attacchi, i cosiddetti ransomware, molte aziende vengono ricattate. Se non si paga, i dati vengono resi pubblici o cancellati. Le aziende devono rispondere a tali richieste?

Assolutamente no. Le aziende non devono permettere ai criminali informatici di ricattarli. Chi paga questi riscatti sostiene questo modello di business e, ancora peggio, il crimine organizzato che c'è dietro. È meglio rivolgersi alla polizia o a noi. Così si può riflettere su come procedere.

Come azienda o privato cosa posso fare per proteggermi da questi attacchi?

È necessario mantenere sempre aggiornato il proprio sistema. Questo significa che, oltre a impostare un firewall, bisogna scaricare gli ultimi aggiornamenti di sicurezza per hardware e software nonché attivare l’ultima versione del programma di protezione dai virus. Se si protegge il proprio computer privato dagli attacchi, si aiutano anche le aziende, perché per gli attacchi alle aziende spesso vengono usati illecitamente i computer privati. È importante anche fare il back-up dei propri dati: così, in caso di attacco, ma anche di un incendio, non andranno persi.

I rischi informatici sono rischi difficili da valutare. Il rapido progresso in ambito digitale rende la valutazione ancora più

complessa. Ma una valutazione dei rischi attendibile e tempestiva è possibile?

In effetti non è semplice. I rischi nei processi aziendali possono effettivamente essere valutati attraverso un’analisi dei rischi. Tuttavia, non si può mai essere del tutto sicuri, ma non è nemmeno ciò che si vuole. Se il rischio fosse pari a zero, l’azienda non potrebbe più essere agile. Inoltre, aziende diverse hanno anche profili di rischio diversi: una start-up può permettersi di correre più rischi rispetto a un’azienda affermata.

> «Costituisce un problema la criminalità informatica organizzata, che rappresenta l’80 percento del crimine in rete. I soli attacchi di ransomware recentemente sono aumentati del 30 percento: si tratta spesso di organizzazioni internazionali.»

Qual è attualmente il pericolo maggiore nella sicurezza informatica?

Non esiste un pericolo maggiore. Costituisce un problema la criminalità informatica organizzata, che rappresenta l’80 percento del crimine in rete. I soli attacchi di ransomware recentemente sono aumentati del 30 percento: si tratta spesso di organizzazioni internazionali. Una stretta collaborazione con le autorità penali estere è quindi importante.

E per quanto riguarda la protezione delle infrastrutture critiche, per esempio la rete elettrica, si può dire che sono ben protette dai ciberattacchi?

Ci sono diversi livelli di evoluzione: alcune infrastrutture critiche sono ben protette, altre devono recuperare terreno. Attualmente stiamo introducendo un obbligo di notifica degli incidenti informatici. In questo modo potremo valutare quali infrastrutture sono le più esposte. Fondamentalmente, però, si può dire che la motivazione di chi effettua gli attacchi deve essere già molto grande per attaccare tali strutture. È molto più facile fare soldi in altri modi.

È possibile assicurarsi contro questi rischi informatici?

Sì, esistono delle assicurazioni cyber. Non posso giudicare quanto siano buone. Per alcune aziende una simile assicurazione può essere interessante. L’importante è che l'assicurazione si attenga alle regole del gioco e che anch’essa non risponda alle richieste di riscatto in denaro, anche se queste ultime dovessero rivelarsi più economiche che sostenere i costi di ripristino dei dati.

Centro nazionale per la cibersicurezza

Il Centro nazionale per la cibersicurezza NCSC è il centro di competenza della Confederazione per la cibersicurezza e di conseguenza il primo servizio di contatto per l’economia, l’amministrazione, gli istituti di formazione e la popolazione per tutte le questioni relative alla cibersicurezza. È responsabile dell’attuazione coordinata della Strategia nazionale per la protezione della Svizzera contro i ciber-rischi. L’NCSC sostiene le infrastrutture critiche nella protezione e nell’elaborazione dei casi. L’NCSC mette pure a disposizione un pool di esperti per fornire supporto agli uffici specializzati nello sviluppo e nell’attuazione

degli standard di cibersicurezza. Inoltre, quale servizio di contatto nazionale riceve le segnalazioni sui ciberincidenti della popolazione e del settore economico, li analizza e dà a chi li ha segnalati una valutazione dell'incidente e raccomandazioni per il seguito della procedura.

Centro nazionale per la cibersicurezza

Che ruolo ha il sistema federale nell'affrontare la sicurezza informatica?

Presenta dei vantaggi e degli svantaggi. Quando si verificano degli incidenti, il coordinamento dei singoli Cantoni nella reazione può essere un po' lento. D'altra parte, ogni Cantone ha i suoi punti di forza: solo per citarne alcuni, Zurigo e Vaud sono forti nel perseguimento penale, il Ticino nella formazione digitale, il Canton Zugo si impegna per i test di sicurezza dei prodotti. Stiamo lavorando per una coesione ancora migliore tra i Cantoni, per renderli così più resilienti di fronte agli attacchi informatici.

A causa della crisi legata al coronavirus, forme di lavoro più flessibili come il telelavoro hanno acquisito sempre più importanza: quali nuove sfide comportano in termini di sicurezza informatica?

Con il telelavoro, la vita privata e quella lavorativa si confondono e questo ha conseguenze anche sulla sicurezza informatica. Spesso, i computer di casa sono usati sia per scopi privati, sia professionali e questo può creare delle falle nella sicurezza attraverso le quali i criminali possono attaccare l'azienda. Pertanto, si dovrebbero distinguere i dispositivi professionali da quelli privati o il datore di lavoro dovrebbe impostare un accesso sicuro all'infrastruttura informatica dell'azienda. Si consiglia anche di bloccare il computer quando non si è alla postazione di lavoro: i bambini sono curiosi e, seppur senza alcuna malizia, potrebbero eventualmente rivelare dati preziosi.

Infine, guardiamo al futuro: si dice spesso che i computer quantistici potrebbero diventare un grande problema di sicurezza perché potrebbero decifrare la crittografia in un istante. Che cosa ne pensa?

Non sono uno specialista di computer quantistici, ma il computer quantistico può a sua volta essere utilizzato per la crittografia, la cosiddetta crittografia quantistica. Su questo abbiamo una ricerca molto interessante in Svizzera. Sarà curioso vedere se con i computer quantistici potremo garantire più sicurezza informatica.

Ritratto

Florian Schütz è il delegato federale alla cibersicurezza. È la persona di riferimento per gli attori politici, gli operatori dei media e la popolazione in caso di domande in materia di cibersicurezza. Dirige il Centro nazionale per la cibersicurezza (NCSC) ed è responsabile dell'attuazione coordinata della Strategia nazionale per la protezione della Svizzera contro i ciber-rischi (SNPC). Florian Schütz ha un master in scienze informatiche e un Master of Advanced Studies in politica di sicurezza e gestione delle crisi conseguito presso il Politecnico federale di Zurigo.

Rischi informatici | Emerging risks | Digitalizzazione | Rischi maggiori

Potreste essere interessati a quanto segue

Add to PDF generator

Gestire i rischi maggiori in modo attivo e in partenariato

I rischi maggiori sono pericoli con potenziale di danno immenso, che si situano in cima alla lista dei rischi della Svizzera.

Focus 04.06.2025

Weiterlesen

Add to PDF generator

«Per molte persone avere la corrente elettrica è scontato»

Maurice Dierick della Società nazionale di rete Swissgrid spiega in un'intervista perché la penuria di energia elettrica è uno dei maggiori rischi per la Svizzera.

Intervista 21.05.2021

Weiterlesen

Add to PDF generator

La crisi legata al coronavirus ha rilevato gravi lacune nella protezione

Il settore assicurativo, finora, come ha affrontato la crisi legata al coronavirus? Il primo bilancio intermedio di Ruedi Kubat (Allianz Suisse) e Ivo Menzinger (Swiss Re).

Contesto 10.06.2021

Weiterlesen