WOW!

Una password sicura deve contenere almeno otto caratteri ed essere costituita da lettere (minuscole e maiuscole), numeri e anche caratteri speciali.

La criminalità informatica ha causato in Svizzera nel 2014 un danno all'economia pubblica pari a circa 200 milioni di CHF.

Il più grande furto di dati di tutti i tempi: alcuni hacker russi hanno rubato nell'estate del 2014 in tutto il mondo 4,5 miliardi di combinazioni di nomi utente e password.

Oracle Java, Adobe Reader o Adobe Flash sono installati sul 99% di tutti i computer. Tutti questi apparecchi sono quindi soggetti ad attacchi informatici.

Anche i social network sono un campo d'azione molto amato dai criminali informatici: fan page falsificate, malware che si diffondono attraverso i clic, o messaggi falsi mirati sono situazioni in cui gli utenti di social network possono facilmente incappare.

La lotta virtuale in Internet è stata visualizzata dall'operatore della sicurezza americano Norse in una mappa interattiva. Questa illustra in tempo reale gli attacchi perpetrati ai danni di diverse istituzioni e aziende in tutto il mondo.http://map.norsecorp.com

SATW
Schweizerische Akademie der Technischen Wissenschaften
Académie suisse des sciences techniques
Accademia svizzera delle scienze tecniche
Swiss Academy of Engineering Sciences

La rivista tecnica per i giovani e per coloro che lo sono ancora

TechnoScope by SATW 3/15

Cyber Security

Internet è un ambiente tutt'altro che salubre. Che cosa può succedere quando si usa il proprio smartphone o apparecchi simili?

Con un concorso

Come funziona il tracking?

Ti sei mai chiesto perché nella ricerca su Google o su altri siti Web vengono richiamati proprio quegli argomenti sui quali hai da poco effettuato una ricerca? Come fa Internet a sapere che io cerco un nuovo impianto stereo o voglio andare in vacanza in Italia? La risposta è semplice: attraverso l'indirizzo IP, tutti i computer e tutti gli smartphone sono chiaramente identificabili. Durante una ricerca, il proprio «indirizzo» è sempre inviato al server che risponderà alla richiesta. Tramite il protocollo HTTP gli amministratori dei siti Web sanno da dove giunge la richiesta e da che tipo di apparecchio.

I webserver, inoltre, raccolgono costantemente dati che riguardano le nostre preferenze. Perlopiù questo avviene di nascosto. Questo «spiare» per scopi di pubblicità o di controllo è chiamato tracking. A tale scopo, nel browser (per esempio Firefox, Safari o Internet Explorer) sono depositati piccoli ritagli di testo, chiamati cookies. Grazie ad essi gli amministratori dei siti possono raccogliere dai siti Web dati che permettono di dedurre l'età dell'utente, il suo sesso, il luogo in cui si trova, la residenza, il datore di lavoro e la nazionalità. Se l'utente comunica anche dati personali, per esempio nell'iscrizione ad un quiz, questi non solo possono essere associati ad un computer, ma anche ad una persona. Questi dati sono poi venduti dagli amministratori dei siti Web a gruppi pubblicitari, interessati ad adattare perfettamente la loro pubblicità ai singoli utenti che navigano in Internet.

Cookies: I siti Web professionali si ricordano che cos'ha cercato un utente in Internet, per esempio un determinato libro. Queste informazioni vengono memorizzate nel browser con piccoli pacchetti di informazioni, i cosiddetti cookies. In occasione di una nuova ricerca su quel sito, il webserver del provider si ricorda, attraverso i cookies presenti nel browser, informazioni concernenti il libro cui l'utente era interessato. Per questo motivo esso appare improvvisamente nella finestra pubblicitaria. I cookies possono essere bloccati o cancellati nelle impostazioni del browser.

App: Molte app sono particolarmente subdole proprio per la registrazione nascosta di dati. Hanno propri canali di comunicazione e determinano persino quali dati siano raccolti e trasmessi sullo smartphone dell'utente, che, nel momento in cui accetta le condizioni generali di contratto del produttore, dà il suo consenso a questa trasmissione. Poiché gli smartphone sono apparecchi molto personali, i fornitori di app possono avere accesso a dati privati. Per esempio a nome dell'utente, indirizzi, numeri di telefono, contatti, agenda, età, sesso e, attraverso la geolocalizzazione e il GPS, la sua posizione in un determinato momento. «Whatsapp», una delle app più amate al mondo, è sempre stata criticata da chi si occupa di protezione dei dati. L'azienda ha anche libera visione di tutte le comunicazioni in corso attraverso l'app.

Like di Facebook: Chi clicca su «like» per commenti o prodotti in Internet, fa sapere a Facebook ciò che realmente gli piace. Per esempio un bel paio di sneaker o determinate posizioni politiche. Facebook combina queste informazioni con i dati del proprio profilo su Facebook e da ciò deduce quali prodotti e offerte possono interessare l'utente. Facebook vende queste conoscenze ai pubblicitari, i quali fanno poi in modo che l'utente di Internet veda possibilmente quella pubblicità, che lo spingerà ad un determinato acquisto.

«Si dovrebbe rivelare la minor quantità di dati possibile in Internet.»

Prof.ssa Solange Ghernaouti, Swiss Cybersecurity Advisory and Research Group, università di Losanna

«Più dati riveliamo di noi, più siamo vulnerabili agli attacchi»

Ciascuno di noi oggi deve proteggersi dalle violazioni in Internet; di questo è convinta Solange Ghernaouti. La professoressa di criminalità informatica dell'università di Losanna spiega nell'intervista perché i criminali informatici non vengono quasi mai presi e perché con i social media noi facilitiamo il loro agire.

Signora Ghernaouti, ci sono già oggi esempi di grandi attacchi di criminalità informatica?
Negli USA la fornitura elettrica di una città è stata attaccata da hacker e paralizzata. La criminalità informatica è oggi un grande pericolo per stati e aziende e dovrebbe essere trattata come tema chiave della politica per la sicurezza nazionale. Quest'estate, inoltre, i dati personali di 37 milioni di utenti del servizio Internet «Ashley Madison» sono stati rubati da ignoti. Si tratta di un Online Dating Service, un servizio di appuntamenti online; gli utenti davano per scontato che i loro dati fossero conservati in modo sicuro e che potessero muoversi nella piattaforma in modo anonimo. Questa si è rivelata una falsa convinzione. Per molte persone ciò ha avuto conseguenze gravi per la vita privata e professionale.

Siamo quindi tutti potenziali vittime della criminalità informatica?
Eccome! In Internet si hanno sempre più casi di truffa. Attraverso Internet è diventato molto semplice per i criminali ricattare e mettere sotto pressione. Tutti oggi sono esposti ad un rischio e la maggior parte degli utenti di Internet non può tutelarsi e difendersi, perché non ha la tecnologia e le conoscenze necessarie. La semplice installazione di un software antivirus oggi non è più sufficiente.

Ma chi in Internet è un po' attento e non incorre in truffe tramite l'e-mail può navigare sicuro, o no?
Non del tutto. Molto oggi accade di nascosto. I dati personali possono essere rubati senza che la persona interessata noti alcunché. È diverso dal caso nel quale si perde il portafoglio e si sa bene quali carte occorre poi bloccare.

Che cosa può fare ciascuno di noi per proteggersi da tali violazioni e furti?
Per non esporsi a rischi inutili, si dovrebbe esibire la minor quantità possibile di dati in Internet. Perché più dati su una persona sono disponibili in Internet, più semplice è per i criminali truffarla, estorcerle denaro o manipolare la sua identità sul Web. I criminali informatici spesso sanno di noi molto più di quanto non sappiamo di noi stessi, grazie alla quantità di dati presenti in Internet. Quindi più usiamo i servizi di Internet e i social media, più ci rendiamo vulnerabili. Questo è molto pericoloso!

Come riesce Lei ad ovviare a questo rischio?
Io utilizzo Internet solo per scopi professionali. Non comunico attraverso i social media e non acquisto tramite Internet. Quindi cerco di mantenere i dati disponibili che mi riguardano più scarsi possibile.

Quanto sono importanti i social media per la criminalità informatica?
Facebook, Twitter, Linkedin e altri servizi sono nel mirino dei criminali informatici, perché le persone qui rivelano molti dati personali.
La maggior parte dei social media non possono garantire la sicurezza dei dati personali.

Come si può rendere il ciberspazio più sicuro?
Dovremmo soprattutto spingere le grandi aziende di Internet a contrastare efficacemente la vulnerabilità dei loro utenti ed eliminare le falle nella sicurezza di sistema. Perché anche se gli utenti di Internet imparano a muoversi in modo cauto e consapevole in Internet, essi non hanno alcun controllo sulle falle della sicurezza di sistema.

«La maggior parte dei social media non possono garantire la sicurezza dei dati personali.»

Quanto è difficile per la polizia intervenire contro i criminali informatici?
Ancora oggi la polizia è quasi impotente. La criminalità informatica non si ferma ai confini statali e le tracce nel ciberspazio possono essere cancellate molto bene. È quindi estremamente importante identificare i creatori di un attacco. I criminali possono essere ovunque nel mondo e irrompere nel mio computer. I privati, inoltre, spesso non osano rivolgersi alla polizia per vergogna. I criminali informatici naturalmente lo sanno e sfruttano la cosa senza scrupoli.

La Svizzera oggi è ben preparata a fronteggiare attacchi informatici?
Non esattamente. Sicuramente aumenta la consapevolezza del problema, ma mancano risorse e misure concrete. Finora sono giunti solo due casi al tribunale federale, anche se sappiamo che ci sono stati molti altri delitti.

Anche Lei stessa è già stata vittima di criminali informatici?
Sì, all'inizio del 2015, dopo l'attacco alla redazione del giornale satirico «Charlie Hebdo» a Parigi, molti siti Web di lingua francese sul tema della sicurezza informatica sono stati attaccati. Anche il mio sito Web è stato bloccato. È stato inquietante, perchè anche questa è una forma di terrorismo. Mi è costato due giorni di lavoro, prima che il sito ritornasse a funzionare.

Infrastrutture cruciali come centrali elettriche e acquedotti, aziende di telecomunicazioni e del traffico, ma anche banche e grandi ospedali, sono sempre più nel mirino degli hacker.

Attacchi critici da Internet

Gli attacchi criminali da Internet sono aumentati in modo notevole negli ultimi anni. A causa della sempre maggiore connessione alla rete, anche importanti infrastrutture sono sempre più colpite. Non tutti sono ben protetti contro questi attacchi.

Alla fine di novembre 2014 due gruppi sconosciuti bloccarono per più giorni l'intera rete aziendale della Sony Pictures Entertainment. Gli aggressori dichiararono di essere in possesso di informazioni confidenziali dell'azienda e minacciarono di pubblicarle. Effettivamente poco tempo dopo cinque film non pubblicati comparvero nelle borse di scambio su Internet. L'americana FBI giunse isn seguito alla conclusione che dietro all'attacco c'era forse il regime nordcoreano, che voleva impedire la pubblicazione del film «The Interview». La commedia tratta di un complotto per l'assassinio del capo di stato nordcoreano Kim Jong-un.

Questi grandi e spettacolari attacchi informatici destano molta attenzione nei media. Eppure sembrano essere sempre l'eccezione, almeno per quanto si sa pubblicamente. Ben più frequenti sono gli attacchi più piccoli e discreti. In questo caso gli aggressori cercano di trovare falle possibilmente non notate nel sistema di difesa, per aver accesso a informazioni delicate o per sottrarre denaro da conti bancari. La cosa perfida è che le persone colpite spesso si accorgono relativamente tardi di essere state attaccate. E quando se ne accorgono, non è per loro sempre semplice riconoscere chi si cela dietro agli attacchi.

Pericoli per la società

Negli ultimi dieci anni sono aumentati anche gli attacchi agli impianti industriali. Leggendario è l'attacco con il worm Stuxnet, con cui nel 2010 hacker americani, o israeliani, hanno danneggiato in modo mirato gli impianti nucleari iraniani. Anche in Germania lo scorso anno c'è stato un caso spettacolare: in un'acciaieria aggressori ignoti sono riusciti a manipolare il software di un altoforno in modo tale da danneggiarlo fortemente.

Attacchi mirati a impianti tecnici possono colpire anche la Svizzera. Per equipaggiare il nostro paese in modo adeguato contro questi attacchi, la Confederazione ha fondato il centro specializzato «Melani». Da un lato gli esperti della Confederazione mettono a disposizione informazioni accessibili al pubblico su come le aziende e i privati possano difendersi. Dall'altro, il centro Melani lavora a stretto contatto con gli amministratori di infrastrutture critiche. In questi casi si tratta di istituzioni il cui funzionamento è indispensabile per la società, come per esempio centrali elettriche o acquedotti, aziende di telecomunicazioni o di distribuzione, ma anche banche e grandi ospedali.

La difesa contro gli attacchi non è ugualmente buona per i vari settori, afferma Pascal Lamia, direttore del centro specializzato. Mentre le banche oggi hanno protetto molto bene la loro infrastruttura IT, le aziende fornitrici di energia elettrica si trovano in una situazione difficile: il settore dell'energia è in pieno rivolgimento, cosa che comporta nuovi rischi. Nuove tecnologie sono continuamente collegate alla rete; nello stesso tempo, le aziende devono risparmiare.

Ospedali difficili da gestire

Secondo Lamia, la situazione è critica soprattutto per gli ospedali. Qui, il collegamento alla rete è aumentato molto rapidamente negli ultimi anni. Un intervento chirurgico, per esempio, non può più essere effettuato senza un'infrastruttura IT funzionante. «Il problema è che negli ospedali sono collegati in rete molti apparecchi che funzionano in modo diverso e che sono protetti in modo altrettanto diverso. Considerando la grande pressione dei costi nel settore della sanità, questa è una grande sfida per ciascun ospedale.»

Lamia individua però il rischio maggiore in un altro settore, vale a dire quello delle piccole e medie imprese: a differenza delle grandi aziende, queste spesso, per ragioni personali e finanziarie, non sono nelle condizioni di proteggersi in modo sufficiente contro gli attacchi. Proprio le piccole imprese sono, infatti, sempre più spesso ricattate dai criminali informatici. Per esempio, gli aggressori minacciano un'azienda che vende prodotti in Internet di bloccare il suo sito Web, se non paga una certa somma di denaro. Sebbene la Confederazione consigli caldamente di non cedere a tali richieste, Lamia sa di aziende che hanno pagato la somma richiesta, perché l'inattività del sito avrebbe causato costi ancora maggiori.

Fattore rischio smartphone

Lo smartphone è sempre più al centro della nostra vita. Ogni giorno mandiamo innumerevoli messaggi attraverso questo pratico apparecchio mobile e vi abbiamo anche memorizzato parecchi dati personali – fotografie, per esempio, o dati delle app sulla salute. Proprio per questo è importante per ciascun utente riflettere sul tema della sicurezza dei dati. Che cosa succede, per esempio, se l'apparecchio viene smarrito o rubato? I dati sono irrimediabilmente persi? E se queste informazioni vanno a finire nelle mani sbagliate?

Nicholas Hansen ha partecipato già tre volte alla Cyber Security Challenge. Alla finale svizzera le squadre non hanno potuto limitarsi a mettere alla prova in diversi modi le loro abilità.

▸ Nicholas Hansen: «Quando si vuole avere successo come hacker, si deve sviluppare una specie di fiuto per individuare dove si potrebbe trovare il punto debole di un sistema ed essere pazienti.»

Un gioco dal retroscena serio

Come ci si protegge contro gli attacchi in Internet? Questa domanda affascina Nicholas Hansen. Il diciannovenne è nella sua fascia d'età uno dei migliori hacker in Svizzera; per questo si è messo alla prova quest'autunno nella Cyber Security Challenge.

Mi sono avvicinato per caso alla Cyber Security, ormai la mia passione. Al secondo anno di tirocinio come informatico avevamo un modulo sulla sicurezza in Internet e l'argomento mi ha immediatamente affascinato. Nel tempo libero ho continuato ad occuparmi da solo di questo tema. Ad un certo momento, un collega mi ha fatto conoscere la «Cyber Security Challenge». Questo fa proprio al caso tuo, ha pensato. E aveva ragione.

Quest'anno era la terza volta che partecipavo a questo concorso per i giovani organizzato dall'associazione Swiss Cyber Storm. Visto il grande numero di partecipanti, la selezione è avvenuta in modo diverso rispetto agli anni precedenti: nella fase di qualificazione ciascuno ha dovuto risolvere alcuni esercizi per conto proprio. Quelli di noi che hanno superato con successo questa fase hanno poi potuto partecipare a metà settembre alla finale svizzera di Sursee. Qui abbiamo dovuto risolvere esercizi complicati in piccoli gruppi, per esempio trovare falle nascoste della sicurezza in applicazioni pubblicitarie, decifrare documenti codificati o trovare l'accesso ad un sistema protetto.

I 10 migliori di noi hanno poi affrontato altre prove: in ottobre abbiamo rappresentato la Svizzera alla finale europea presso il KKL di Lucerna. Qui abbiamo affrontato squadre provenienti da Germania, Austria, Inghilterra, Spagna e Romania. Ogni squadra era composta da dieci membri e aveva un proprio webserver a disposizione, su cui erano caricate applicazioni con determinati punti deboli. Il nostro compito era quello di mettere in sicurezza queste applicazioni ed eliminarne i punti deboli. Allo stesso tempo dovevamo cercare di penetrare nel server delle squadre concorrenti.

Per questa finale la mia squadra si è preparata intensamente. Abbiamo creato un archivio centrale in cui abbiamo depositato tutti i nostri tool e abbiamo istituito un canale chat comune. Abbiamo discusso e assegnato un compito a ciascun membro della nostra squadra. Io ero responsabile di riconoscere tempestivamente gli attacchi dalle altre squadre. È stato interessante vedere come gli altri ci attaccavano, perché questo ci dava indicazioni su come potevamo violare i loro sistemi. Purtroppo questo non è bastato per vincere. Siamo arrivati terzi.

Al momento mi occupo del tema Cyber Security soprattutto nel mio tempo libero. Per me è tutto una specie di gioco: mi diverte moltissimo risolvere problemi, attaccare gli altri e difendermi con destrezza contro eventuali attacchi. Dopo che ho risolto un problema complicato, mi sento bene. E se non ce la faccio subito con le mie idee, è certamente un po' frustrante, ma allo stesso tempo mi sprona ad andare avanti. Quando si vuole avere successo come hacker, si deve sviluppare una specie di fiuto per individuare dove si potrebbe trovare il punto debole di un sistema. Quando per esempio vedo in un sito web più vecchio un modulo di input, mi interessa subito vedere se l'infrastruttura dietro questo modulo mostra qualche punto debole. Oppure, quando in un programma è memorizzata una password in forma codificata, desidero scoprire dove esattamente ciò sia effettuato e in base a quale modello avvenga la codifica.

Se si vuole avere successo come hacker, si deve avere pazienza e provare sempre nuove cose. Purtroppo, di solito il tempo passa molto velocemente e succede sempre che rimango davanti al computer fino a troppo tardi di notte. Qualche volta ho bisogno di più giorni per risolvere un problema. Allora non è molto semplice per me staccare. Mi riesce meglio quando finisco subito con una buona idea. Così non ho la tentazione di andare ancora avanti.

Attualmente lavoro ancora presso la mia azienda di tirocinio. In qualità di informatico, sono responsabile del funzionamento dell'infrastruttura IT interna. Dopo la scuola reclute probabilmente studierò informatica all'università. Mi immagino di lavorare poi nel settore della sicurezza in Internet, perché è un settore molto importante per la società. Oggi sempre più apparecchi e impianti che devono funzionare in modo affidabile sono collegati in rete fra loro. In questo modo, ovviamente, aumenta il pericolo che siano bloccati a causa di attacchi informatici. Se sappiamo dove sono i punti deboli possiamo proteggere meglio questi impianti.

Ah, ecco!

Ah, ecco: come funziona la codifica?

Attraverso la codifica, un cosiddetto testo in chiaro, vale a dire un testo normalmente leggibile, è trasformato in un «testo segreto» che apparentemente non ha senso. Già nell'antico Egitto, messaggi importanti erano riscritti in testi segreti per evitare che potessero essere letti, nel caso che durante la trasmissione fossero finiti in mani sbagliate. Oggi la codifica serve soprattutto per la trasmissione sicura di informazioni attraverso canali digitali come Internet. Quindi la codifica di e-mail permette che messaggi confidenziali possano essere inviati dai mittenti ai destinatari, impedendo che qualcun'altro possa leggerli. A tale scopo è necessaria infatti una «chiave». Nelle moderne procedure di codifica con computer, essa è costituita da una sequenza di bit, quindi un numero molto lungo composto da zeri e uno. Oggi le procedure di codifica più usate possono contare su una relativa sicurezza. La quantità di calcoli necessari per scoprire una chiave è così elevata che questa non può essere trovata in un tempo ragionevole e con strumenti di calcolo comunemente in uso.

Simmetrica o asimmetrica

In linea di massima si distinguono due tipi di codifica: i processi di codifica simmetrica utilizzano la stessa chiave segreta per la codifica e la decodifica. Nella codifica asimmetrica, invece, per la codifica del testo in chiaro è utilizzata una chiave diversa da quella della decodifica del testo segreto. A tale scopo, la chiave per la codifica è pubblica, vale a dire nota anche ad altri utenti. La chiave per la decodifica è invece segreta.

La crittologia è una scienza che si occupa della sicurezza delle informazioni. In essa rientrano i settori specialistici della crittografia, che si occupa del processo di codifica, e della crittoanalisi, che si dedica alla decifratura di sistemi di codifica.

www.satw.ch/concorso

Formazione

Chi desidera diventare esperto nel settore della Cyber Security deve avere ottime conoscenze informatiche. I corsi di studi in informatica in Svizzera sono offerti dalla formazione professionale di base, da scuole universitarie professionali e dalle principali università, inclusi i politecnici di Zurigo e di Losanna.

Una panoramica delle possibilità di formazione si può trovare su
www.orientamento.ch nei capitoli Scelta professionale> Scuole e formazioni> informatica

Le professioni nel settore della sicurezza – quindi anche per aspetti della sicurezza nel mondo reale – si possono trovare in tedesco su
www.berufsberatung.ch nei capitoli Berufswahl> Berufe und Ausbildungen cercare Sicherheit.

Concorso

Che cosa sai della Cyber Security? Metti alla prova le tue conoscenze, partecipa al concorso e puoi vincere tre buoni della Digitec del valore di 150 CHF. Con il buono puoi, per esempio, acquistare un programma di sicurezza, in grado di proteggere il tuo computer dagli attacchi informatici, o molte altre cose interessanti. Il concorso è aperto fino al 30 aprile 2016.
www.satw.ch/concorso

Impressum

SATW Technoscope 3/15, dicembre 2015
www.satw.ch/technoscope

Idea e redazione: Beatrice Huber
Collaboratori di redazione: Felix Würsten, Samuel Schläfli
Foto: Fotolia, Swiss Cyber Storm, Nicholas Hansen, Solange Ghernaouti

Abbonamento gratuito e ordini supplementari
SATW, Gerbergasse 5, CH-8001 Zurigo
technoscope@satw.ch, Tel +41 (0)44 226 50 11

Technoscope 1/16 uscirà a maggio 2016 e avrà per argomento «La galleria di base del San Gottardo»