Impedire la cibercriminalità

Manuale per piccole e medie imprese

Editoriale

Polizia cantonale di Berna e Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI su incarico della Rete assistenza indagini lotta alla criminalità digitale (NEDIK). Contatto: Polizia cantonale di Zurigo, NEDIK, Zurigo, cyc_nedik@kapo.zh.ch

Immagini: messe a disposizione dalla Polizia cantonale di Zurigo.

Ihre **POLIZEI**
Votre **POLICE**
La vostra **POLIZIA**

Kantonale und Städtische Polizeikorps
Corps de police cantonaux et municipaux
Corpi di polizia cantonali e comunali

Indice

1 Gli attacchi cibernetici costano, anche a Lei?

La digitalizzazione apre nuove opportunità di crescita e possibilità d'impiego per l'economia. Ciò significa pure, tuttavia, una crescente dipendenza da una funzionante infrastruttura informatica digitale. Determinati criminali ne approfittano in pieno. Dall'azienda artigianale fino a grandi imprese con parecchie migliaia di collaboratori – ognuno ne può essere vittima. Già il 40 percento delle imprese svizzere che hanno partecipato a un'inchiesta hanno indicato di avere sofferto di cibercriminalità.[1] Nei fatti, non soltanto possono finire offline i siti web, ma può rimanere colpita l'intera rete informatica di un'impresa. Il più delle volte le imprese subiscono danni finanziari e in molti casi vengono rese pubbliche anche informazioni riservate.

Ci si può proteggere da molte cyberminacce.

Col presente materiale informativo, la polizia e la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) intendono dare raccomandazioni concrete per la protezione dalla cybercriminalità e visualizzare come procedere nel caso di un'aggressione avvenuta. Inoltre, vogliamo incoraggiarla a notificare alla polizia casi rilevanti che possano coinvolgerla. Soltanto l'unione fra l'autorità della giustizia penale e l'economia permette di scoprire e condannare i colpevoli e così combattere la cybercriminalità in modo sostenibile.

Informazioni approfondite sulla Sua sicurezza IT le trova su www.melani.admin.ch

1 «Globale Umfrage zur Wirtschaftskriminalität 2018 – Schweizer Erkenntnisse», PwC, 2018.

2 Come i cyberaggressori ottengono i Suoi soldi

Nel caso di cyberattacchi, i perpetratori spesso procedono secondo gli stessi modelli e utilizzano sempre gli stessi mezzi. Questi si lasciano suddividere grosso modo nelle categorie ricatto, truffe e abuso di dati.

2.1 Come La ricattano

I ricattatori attaccano l'infrastruttura informatica delle vittime con l'obiettivo di estorcere dei soldi. Il tentativo comporta il disturbo se non addirittura il blocco di possibilmente tanti processi dell'impresa. Le vittime vengono contattate con la pretesa di dovere versare una somma di danaro per fermare l'attacco o impedire la pubblicazione di dati rubati.

Gli aggressori conoscono la natura e la dimensione dell'impresa che si prestano ad attaccare.

Ransomware	Si inviano file nocivi a vasto raggio, ad esempio tramite e-mail, per rubare informazioni e password. Le potenziali vittime trovate con questo metodo vengono poi spiate specificamente per raccoglierne informazioni. Se i perpetratori hanno successo, prendono il controllo e incominciano a cifrare i dati dell'impresa. In certi casi rubano anche i dati stessi. I ricattatori chiedono un riscatto (ransom in inglese) per decrittare di nuovo i dati estorti.
DDoS (aggressione per sovraccarico)	Un sistema accessibile via internet viene sovraccaricato con moltissime interrogazioni in modo da non poter più adempiere al suo vero compito. Per fermare l'attacco occorre pagare un riscatto. I perpetratori però possono essere anche gruppi intenzionati a nuocere all'impresa od organizzazione, oppure competitori che vogliono procurarsi un vantaggio sul mercato.
Pubblicazione di dati	I ricattatori minacciano di rendere pubblici dati precedentemente sottratti all'impresa se non ottenessero un riscatto.

2.2 Come La truffano

I truffatori tentano con l'inganno di persuadere la vittima a fare qualcosa che in fondo non vorrebbe. Spesso si sceglie uno scenario che risvegli possibilmente tante emozioni nella persona presa di mira o che le sia familiare. La familiarità induce un falso senso di sicurezza.

Spesso i delinquenti si informano preventivamente al reato sulla struttura dell'impresa. Ciò avviene attraverso informazioni liberamente accessibili (ad esempio sul sito aziendale o nelle reti sociali). Poi si prende di mira una persona adatta e la si confronta con uno sceneggiato ritagliatole su misura. Il termine tecnico del metodo utilizzato dai perpetratori allo scopo è social engineering. Tramite il social engineering si persegue lo scopo di far eseguire alla vittima atti pilotati occultamente a distanza dai perpetratori senza che la vittima stessa ne sia del tutto cosciente.

Gerarchia	I delinquenti approfittano della struttura gerarchica dell'impresa e creano una certa pressione ad agire. Ad esempio, simulando l'identità di un superiore ed esortando un collaboratore o una collaboratrice nel nome del superiore a rendere pubbliche determinate informazioni oppure a eseguire un bonifico.
Tempo ristretto	Alle vittime viene fatto credere di stare sotto tempo ristretto per una scadenza.
Brama / curiosità	Alla vittima viene promessa un'utilità o una gradita sorpresa se si apre il file o se si clicca sul link presentato.
Paura / collera	Si minacciano conseguenze sgradite se non viene eseguito l'ordine. Oppure si rilasciano dichiarazioni evidentemente false che possono essere chiarite con un clic sul link.
Compassione	Il tema presentato interessa emotivamente la vittima. Ad esempio, la vittima vuole impegnarsi nell'eliminazione di mali sociali.

2.3 Come abusano dei Suoi dati

Spesso si ritirano soldi dal conto della vittima attraverso software nocivo. Ma si può guadagnare molto anche con la vendita sul mercato nero dei dati di accesso rubati.

Obiettivo del reato per lucro sono talvolta anche dati aziendali. In questo caso si tratta principalmente di segreti aziendali o dati della clientela. Se la Sua ditta salva dati di accesso dei clienti o persino dati delle loro carte di credito, potrebbe essere di grande interesse per la cyberdelinquenza.

I dati vanno salvati e conservati con metodi di sicurezza speciale (cifrati).

Trojan e-banking	I trojan e-banking sono programmi che permettono all'aggressore un accesso ai Suoi dati dell'e-banking. Spesso i trojan vengono spediti per e-mail, ad esempio camuffati da fattura o candidatura.
Fuga di dati	Gli aggressori si procurano l'accesso alla Sua rete aziendale. Se trovano dati utili ai loro scopi, li ricopiano. Dopo di che possono venderli a terzi oppure ricattare l'impresa con la minaccia di renderli di dominio pubblico.
Phishing	Il phishing è una tecnica per arrivare a dati riservati. I suoi veicoli sono ad esempio l'e-mail, siti web, telefonia via internet o messaggi sms. I riceventi vengono avvisati che i loro dati non sono più sicuri o attuali e che si lasciano aggiornare seguendo il link pubblicato in calce. Il link però collega a un falso sito internet. Le vittime accedono, e così i perpetratori ottengono dati di accesso che permettono ad esempio di acquistare merci contro fattura.

3 Come può proteggere la Sua impresa

Per sventare una cyberaggressione servono determinate misure tecniche e organizzative. Queste azioni non possono essere delegate a collaboratori subordinati ma vanno affrontate, realizzate e coordinate dal management dell'impresa.

Le misure contro le cyber-aggressioni vanno affrontate a livello di management.

3.1 Con misure di protezione tecniche

> **Esegua update di sicurezza**
Il software antiquato è un portone spalancato come lo preferisce il software dannoso. Si accerti che tutti i computer e server nella Sua rete carichino automaticamente gli aggiornamenti di sicurezza. Aggiorni permanentemente pure applicazioni di terzi come Adobe Reader, Adobe Flash e Java. Ciò vale pure per apparecchi periferici come stampanti, router ecc.

Se la Sua impresa possiede una presenza web, si accerti che un Content Management System (CMS), cioè il sistema di gestione del sito eventualmente inserito, sia tenuto continuamente aggiornato. La maggior parte dei CMS dispongono di una funzione di aggiornamento automatico semplice da attivare.

> **Utilizzi un firewall**
Dovrebbe inserire un firewall personale in tutti i computer. Protegga inoltre la Sua rete aziendale da internet tramite firewall. Questo dovrebbe bloccare in modo standardizzato tutto il traffico con internet all'infuori dello scambio di dati liberato tramite regole prestabilite.

Suddivida la Sua rete aziendale in singoli settori. Per esempio: reti separate per produzione, personale e contabilità. Non esiste alcun motivo per l'accesso agli impianti di produzione da parte dell'ufficio del personale. Così sventa il pericolo che, ad esempio, dei computer di controllo degli impianti non aggiornabili diventino dei comodi portoni d'entrata per aggressori.

Metta in sicurezza il Suo accesso remoto: non si limiti a proteggere l'accesso remoto alla rete aziendale soltanto con una semplice autentificazione (nome utente e password). Utilizzi almeno un'autentificazione bifase oppure acceda tramite una rete privata virtuale (Virtual Private Network – VPN). Ciò vale pure per l'accesso da parte di servizi IT e amministratori esterni.


PASSWORD

> **Protegga i Suoi dati**
Definisca una procedura che regoli periodicamente la messa in sicurezza dei dati e si attenga conseguentemente a una regolarità fissa. Consideri quante giornate di perdita dati potrebbe sopportare nel caso di avvenimento blackout e salvi una rispettiva copia supplementare del Suo backup separatamente (offline) e fuori sede (offsite). Si eserciti di tanto in tanto nell'inserimento dei backup per esserne pratico se mai si trovasse nella necessità di farlo in caso di emergenza. Si accerti di custodire la rispettiva versione di backup precedente per un periodo di alcuni mesi.

> **Installi un antivirus**
Si accerti che su ogni computer sia installato un antivirus e che la protezione in tempo reale sia attivata. Abbia anche cura che esso si aggiorni regolarmente a scadenza periodica e che svolga un'intera scansione di sistema quotidiana.

> **Cautela nell'utilizzo di servizi cloud**
Sia cauto nell'utilizzo di servizi cloud. Il loro uso è inserito in numerosi programmi. Valuti quali dati salvare localmente e quali sul cloud. Eviti sempre comunque di classificare dati sensibili e segreti aziendali nel cloud senza cifrarli preventivamente.

Importante è la precauzione!
Rifletta preventivamente su quali misure adottare nel caso di probabili aggressioni future. Definisca quali siano i log file (file di registro eventi) da salvare e per quanto tempo farlo. Computer e server sono in grado di verbalizzare tutti i processi di sistema rilevanti oppure i dati di collegamento con altri computer. Nel caso ideale ciò avviene in un luogo centralizzato. Numerosi dati log non soltanto assistono le autorità della giustizia penale nelle loro inchieste, ma aiutano pure l'impresa a riconoscere l'origine di un'aggressione, a ottenere informazioni su sistemi infetti nella propria rete e a prendere contromisure adeguate. Se la Sua rete dovesse essere amministrata da un'impresa di servizi IT, Le consigliamo di discutere con essa le questioni dei log file e del riconoscimento di possibili aggressioni. Raccomandabile è pure l'inventariazione attualizzata e completa di tutti i sistemi, software e reti presenti.

3.2 Con misure di protezione organizzative

> **Regoli la gestione delle informazioni aziendali**
Definisca le direttive per l'inoltro d'informazioni aziendali. Consideri in maniera precisa quali informazioni, per esempio, siano da pubblicare sul Suo sito web o nei media sociali perché tali dati vengono raccolti da delinquenti. In linea di massima nessuna informazione confidenziale dovrebbe essere trasmessa tramite canali anonimi (ad esempio telefono o e-mail).

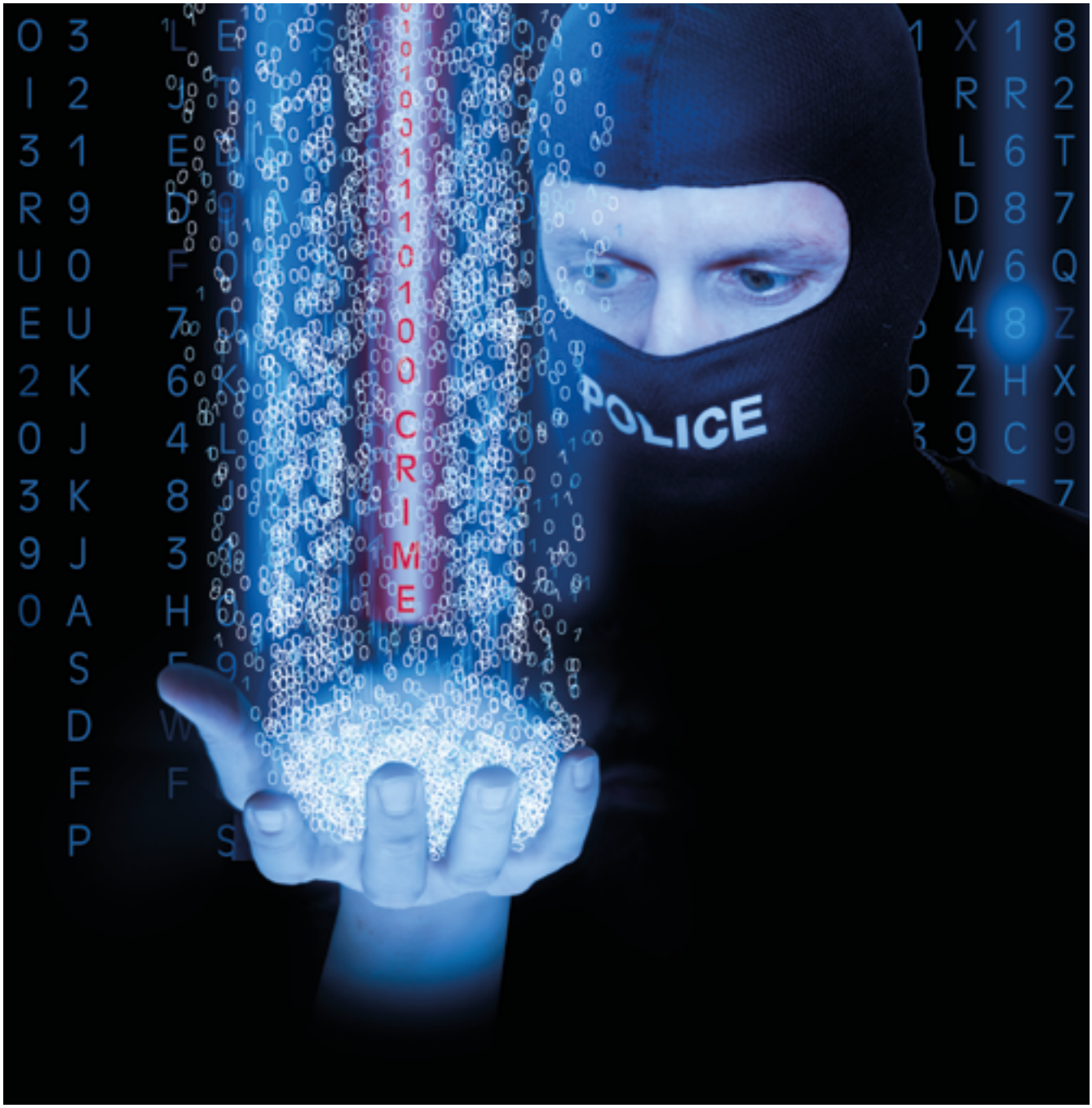
> **Sensibilizzi i Suoi collaboratori nel trattamento delle e-mail**
Spesso elementi informatici nocivi arrivano sui Suoi computer via allegati camuffati da pretese fatture. Mantenga una sana diffidenza; non scansi all'occorrenza una richiesta di chiarimento telefonica e sensibilizzi pure i Suoi collaboratori. Si accerti assolutamente che nessuna macro possa essere eseguita da documenti Microsoft di provenienza incerta.

> **Utilizzi password sicuri e non le divulghi**
Definisca regole vincolanti per password e le implementi rigorosamente. La lunghezza minima di una password dovrebbe essere di dodici caratteri e comprendere sia lettere sia cifre sia anche caratteri speciali. Disponga sempre quando possibile un'autentificazione a due fattori. Eviti assolutamente l'utilizzo ripetuto della stessa password. Utilizzi invece un password manager e generi una propria password per ogni applicazione. Sul mercato trova vari sistemi di password management per i diversi sistemi operativi e computer; esistono programmi sia gratuiti che brevettati a pagamento. Non divulghi incondizionatamente mai password e dati di accesso per e-mail o telefono.

> **Regoli l'accesso ai dati**
I collaboratori generalmente non dovrebbero disporre di diritti da amministratore. Ai collaboratori vanno concessi solo i diritti che servono per eseguire i compiti loro assegnati.

> **Protegga il Suo conto bancario online**
Per i pagamenti, utilizzi un computer separato che non serva a navigare su internet o a ricevere e-mail. Tutte le procedure riguardanti le operazioni di pagamento sono da regolamentare chiaramente all'interno dell'azienda e da adempiere in ogni caso da parte di tutti i collaboratori attraverso, ad esempio, il principio del doppio controllo e la firma collettiva. In base a questi sistemi, i pagamenti devono essere vistati da un altro utente e-banking legittimato prima di essere inviati. Ciò vale soprattutto quando sono più collaboratori a essere autorizzati a effettuare pagamenti online. Si rivolga alla Sua banca in merito a possibili misure di sicurezza.

> **Collaborazione con un'impresa di servizi IT**
Mentre le grandi imprese dispongono spesso di propri reparti IT, molte delle più piccole dislocano le rispettive mansioni. Si accerti che le competenze in merito alla sicurezza IT siano chiaramente regolate fra Lei e l'impresa di servizio. Ciò riguarda specialmente le misure tecniche e organizzative sopra descritte. Stabilisca per contratto l'attribuzione della responsabilità in caso di sinistri se derivassero dall'inosservanza delle misure di sicurezza pattuite.


POLICE
CRIME

4 Come può contribuire anche Lei al successo delle indagini di polizia per scoprire i colpevoli

4.1 Ogni denuncia può essere decisiva

La polizia non è interessata ai Suoi segreti d'impresa e non interferisce nella Sua infrastruttura. Nel caso di un'aggressione si limita a cercare informazioni e tracce rilevanti ai fini dell'indagine sul reato. L'indagine stessa sottostà al segreto di ufficio. Mancano di fondamento eventuali timori di conseguenze negative in seguito alla denuncia avvenuta, ad esempio in merito al sequestro di computer aziendali per un periodo prolungato oppure alla pubblicazione di un caso. La polizia La prende molto sul serio e discute eventuali azioni penali preventivamente con l'impresa prima di applicarle. Nella maggior parte dei casi si può trovare un modo di procedere che funzioni per ambedue le parti.

Indagini nel cyberspazio sono una sfida particolare, anche perché dietro molti casi si nasconde una delinquenza internazionale. Tuttavia, si riesce anche a ottenere dei buoni successi. L'esperienza ci dice che molti reati nel cyberspazio sono in relazione fra di loro e mostrano delle similitudini. Ogni denuncia può perciò fornire l'indicazione decisiva per scoprire i perpetratori.

4.2 Denunci il fatto senza indugio

Se venisse a scoprire un reato dovrebbe informarne al più presto possibile la polizia o il pubblico ministero. Quanto più tempo aspetta, tanto maggiore è la probabilità di cancellare tracce valide. Inoltre, ogni interferenza può avere come effetto che le tracce diventino inutilizzabili o spariscano. Qualunque posto di polizia accetta la Sua denuncia orale o scritta. Sul portale della polizia svizzera www.suisse-epolice.ch trova il numero di telefono del posto di polizia a Lei più vicino.

4.3 Procedura per una notifica senza denuncia penale

Alcune ditte in determinate situazioni rinunciano a una denuncia. Per questi casi si è creata la possibilità d'inoltrare delle informazioni alle autorità competenti da parte delle vittime. A questo scopo inoltri nell'eventualità un'informazione a MELANI sotto www.melani.admin.ch. Agli organi inquirenti è possibile, grazie a queste informazioni, mantenere una migliore visione d'insieme sulla situazione di minacce attuali e su reati simili o di stessa categoria, così come ridurre il numero di casi ignoti. Queste notifiche però non danno adito a una denuncia penale, rispettivamente non possono essere utilizzate in tribunale in caso di processo.

5 Cosa deve fare se il fatto accadesse nonostante tutto

Pronto soccorso nel caso di un cyberattacco
Nonostante tutte le misure cautelari Le può accadere di essere vittima di una cyberaggressione. È perciò importante che sappia cosa fare in questo caso.

1. Isolare
   > Scolleghi tutti i sistemi immediatamente dalla rete. Non dimentichi di spegnere il WLAN.
   > Per il reboot dei sistemi aspetti fino a che la polizia non abbia messo in sicurezza le tracce.

2. Contattare
   > Contatti senza indugio la polizia. Gli specialisti La consiglieranno e L'assisteranno nella procedura, metteranno al sicuro le tracce e indagheranno. Su www.suisse-epolice.ch trova il numero di telefono del posto di polizia a Lei più vicino.
   > Specialisti di imprese private l'assisteranno nella riparazione della Sua infrastruttura e se necessario nella ricostruzione della stessa.
   > Notifichi aggressioni tentate ma senza danni a MELANI.


JDF LOR9 D9AA9Q3O
HJO JU9UO FOSD2A2I
E3A DWEU 70OIOPOE
WL SE2K 6KLJIJ1U
L3 J80J 4LQAODSO
3L F 3K 8J2SJSJ2
KS 3 9J 319U1 A3
HD S 0A H01DL L9
F0 6 S E9LAH SO
HE L D W07JW K1
D3 0 F FDJ J J