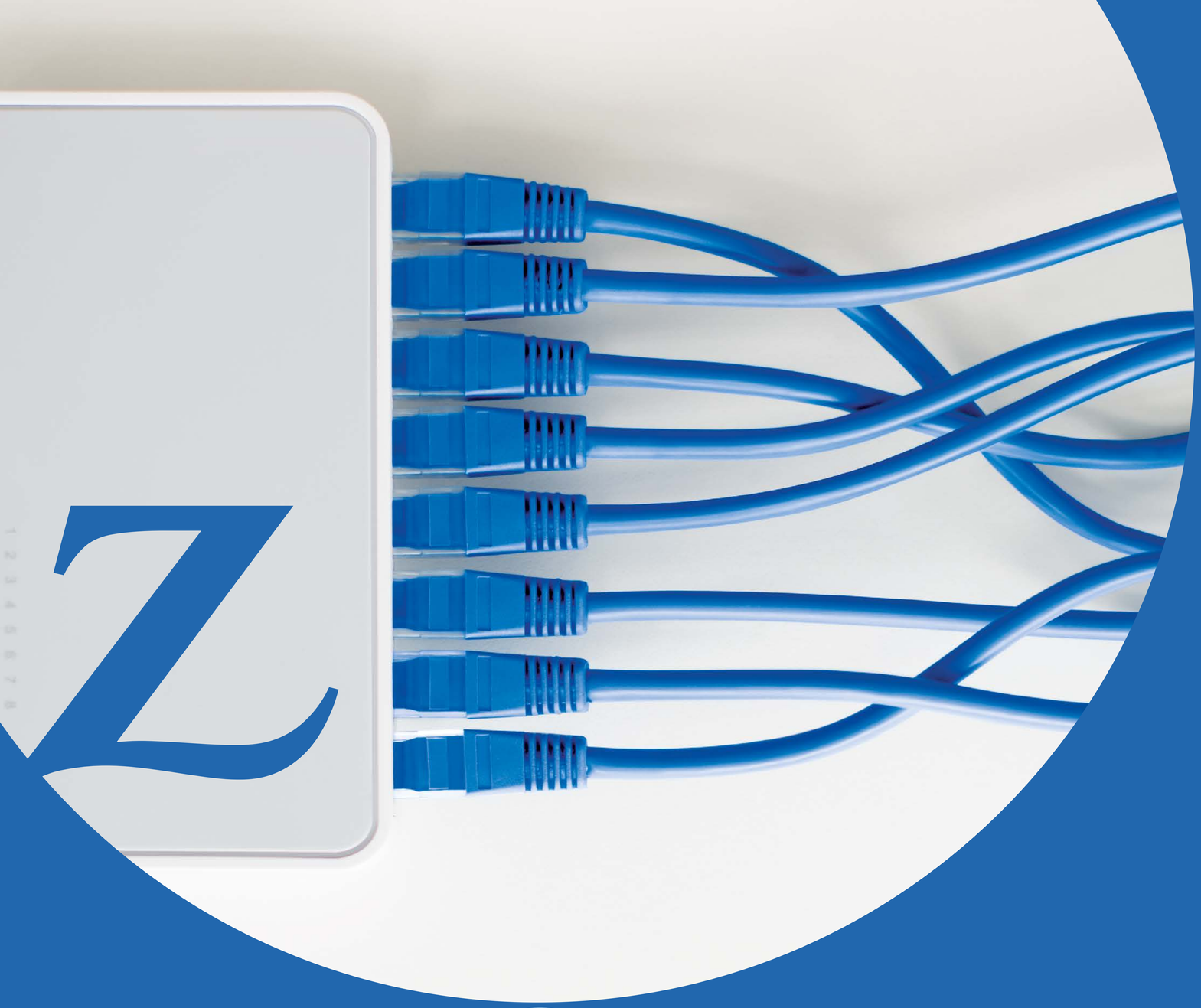


ZURICH

Opuscolo sui rischi informatici

Indice

Digitalizzazione: opportunità e rischio nello stesso tempo

La svolta digitale offre enormi opportunità alle PMI svizzere, che possono semplificare i processi esistenti, ottimizzare prodotti e servizi e creare così valore aggiunto per la propria clientela. Questa svolta spesso richiede l'intera attenzione da parte della direzione aziendale. Di conseguenza, i rischi di natura informatica passano sovente in secondo piano e vengono trascurati. Eppure è di grandissima importanza proteggersi dai rischi informatici, affinché gli imprenditori possano sfruttare il potenziale offerto dalla digitalizzazione e restare protetti da effetti secondari indesiderati.

La Consigliera nazionale Doris Fiala, Presidente dei Swiss Cyber Security Days, ne è convinta: «La digitalizzazione è un'enorme opportunità, ma presenta anche alcuni rischi». Secondo Fiala, dalle stime emerge che ogni anno i costi imputabili alla criminalità informatica ammontano a 5 miliardi di franchi nella sola Svizzera: «Più del bilancio dell'esercito». Molte PMI svizzere non si rendono ancora conto di essere a rischio, ha osservato Doris Fiala. «Le PMI devono prestare molta attenzione ai costi per far fronte alla concorrenza quotidiana e pertanto risparmiano sulla sicurezza in Internet. Tuttavia, proteggersi bene a tutti i livelli conviene».

La rilevanza dei rischi informatici per le PMI è attestata anche da un recente sondaggio dell'istituto gfs-zürich. Degli oltre 500 direttori commerciali consultati, un quarto ha dichiarato di essere già stato vittima di un attacco informatico con serie conseguenze

Digitalizzazione: opportunità e rischio nello stesso tempo

La digitalizzazione comprende tutti i rami: in quasi tutte le imprese la maggior parte delle comunicazioni e del lavoro d'ufficio quotidiani si svolgono con il supporto di computer. A seconda del tipo di attività, poi, le imprese presentano anche altre aree soggette ad attacchi:

Libere professioni come architetti e ingegneri
Sviluppo, pianificazione e calcolo si svolgono oggi in modo del tutto computerizzato, ad es. mediante l'impiego di programmi CAD. Senza un'infrastruttura IT funzionante tutti i lavori si fermano.

Commercio e logistica
Ordini, gestione del magazzino e vendita sono amministrati attraverso sistemi ERP. Anche i processi di vendita ai clienti finali si svolgono sempre più frequentemente tramite Internet.

Settore alberghiero, gastronomico e dell'intrattenimento
Ordini e pianificazione dell'impiego del personale, nonché tutti i lavori amministrativi, vengono svolti tramite software specializzati. Prenotazioni e ordini avvengono sempre più frequentemente online, in parte anche tramite app.

Servizi finanziari:
Praticamente tutte le transazioni sono completamente digitalizzate versamenti, negoziazione di titoli e persino ipoteche sono sempre più spesso stipulati e rinnovati online.

Sanità, assistenza e ambito sociale
I trattamenti e la gestione dei pazienti sono pianificati e supportati da sistemi di informazione centralizzati. Sempre più spesso i dossier dei pazienti sono disponibili in formato digitale e agevolano il lavoro del personale sanitario. Senza questi sistemi oggi funziona ben poco.

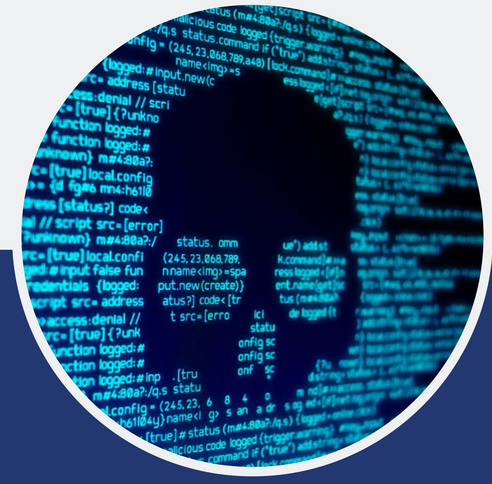
Produzione
I processi produttivi sono già in gran parte, a seconda del ramo dell'azienda, gestiti tramite impianti automatizzati e robotica. Senza una gestione funzionante di questi impianti la produzione si arresta.

Trucchi tipici degli hacker

Modelli d’attacco

Le rapine in banca appartengono al passato. Al giorno d’oggi chi vuole accedere a grandi somme di denaro non ha più bisogno del piede di porco, della pistola e un’automobile su cui fuggire. Gli servono piuttosto un buon collegamento a Internet, un’intelligenza acuta e molta energia criminale. Le forme di attacco più utilizzate dai criminali informatici sono:

- blocco d’infrastrutture IT
- furto di dati
- denial of service
- frode informatica



Porte d’accesso

Ma come riescono i criminali informatici ad accedere alle infrastrutture IT per sferrare i loro attacchi? Nonostante i comuni metodi di attacchi informatici siano noti, in molti casi hanno ancora successo. Le «porte d’accesso» più comuni includono:

- accesso a distanza
- phishing
- infezione drive-by
- sistemi non aggiornati o configurazioni errate
- parti terze (ad es. fornitori di servizi esterni)

Trucchi tipici degli hacker

Modelli d' attacco Porte d' accesso

Le rapine in banca appartengono al passato. Al giorno d'oggi chi vuole accedere a grandi somme di denaro non ha più bisogno del piede di porco, della pistola e un'automobile su cui fuggire. Gli servono piuttosto un buon collegamento a Internet, un'intelligenza acuta e molta energia criminale. Ma in che modo concretamente gli hacker raggiungono il loro obiettivo? Nonostante la varietà e la raffinatezza degli attacchi informatici, la maggior parte dei casi di sinistro che si verificano quotidianamente risponde a pochi comuni modelli:

Blocco d' infrastrutture IT

Gli hacker riescono ad accedere alle infrastrutture IT e le bloccano. Un mezzo comune è in questo caso il cosiddetto «ransomware», ovvero «software per il riscatto di denaro», ed in effetti è proprio di questo si tratta: la persona che effettua l'attacco introduce un programma per la cifratura di dati e programmi nelle infrastrutture IT (ad es. controller di dominio di Windows, sistemi ERP). Successivamente contatta la sua vittima, informandola che solamente dietro pagamento di un riscatto fornirà la chiave digitale per decodificare e quindi sbloccare i dati e i programmi. Spesso l'hacker riesce a eseguire la cifratura, oltre che dei sistemi operativi, anche di quelli di back-up, e di conseguenza per molte vittime non ci sono alternative e si rassegnano a pagare il riscatto.

Furto di dati

Coloro che effettuano gli attacchi informatici riescono ad accedere alle infrastrutture IT in cui sono presenti dati sensibili e ne sottraggono una copia. Particolarmente preziosi per gli hacker sono i dati dei clienti, che possono essere utilizzati per vari tentativi di frode. Ciò vale in particolare per i dati delle carte di credito o le informazioni con le quali è possibile falsificare le identità (ad esempio le copie dei passaporti).

Trucchi tipici degli hacker

Modelli d' attacco Porte d' accesso

Denial of Service

Gli hacker bombardano i canali di comunicazione elettronici delle aziende con milioni di richieste. Di conseguenza, i sistemi colpiti (ad esempio pagine Internet o sistemi di telefonia voice-over-IP) vengono sovraccaricati e smettono di funzionare. Generalmente per questo tipo di attacchi gli hacker utilizzano reti di bot, ossia migliaia di computer privati oppure anche di elettrodomestici precedentemente hackerati, che poi dietro comando accedono contemporaneamente a tutti questi canali di comunicazione della vittima. Successivamente, nella maggior parte dei casi, vi è una richiesta di riscatto: se l'impresa colpita non vuole subire altri attacchi deve pagare.

Frode informatica

Gli hacker utilizzano canali di comunicazione elettronici per indurre i collaboratori a effettuare versamenti di denaro che vanno ad arricchire gli hacker stessi. In questo caso, solitamente si simulano scenari di crisi: il soggetto che effettua l'attacco finge di essere il CEO, il CFO o un altro dirigente dell'impresa. Spesso in questo contesto si utilizzano account e-mail compromessi. Si tratta di account e-mail di cui gli hacker si sono impossessati dopo aver sottratto nomi utente e password. Questa frode prende anche il nome di Business Email Compromise (BEC).

Trucchi tipici degli hacker

Modelli d' attacco **Porte d' accesso**

Indipendentemente da quale dei suddetti attacchi abbia luogo, è necessario agire rapidamente per limitare i danni. Inoltre, sarebbe opportuno ridurre il rischio di incidenti futuri adottando apposite misure tecniche od organizzative. Nonostante i comuni metodi di attacchi informatici siano noti, in molti casi hanno ancora successo. Nella prossima sezione sono descritte le più comuni «porte di accesso» dei criminali informatici, che spesso consentono anche più di una forma di attacco:

Accesso a distanza

Nel periodo del coronavirus molte aziende hanno dato ai loro collaboratori la possibilità di poter accedere al sistema aziendale tramite home office: un vero e proprio invito a nozze per i criminali informatici di tutto il mondo. Infatti, una sicurezza elevata è garantita solamente da quelle tecnologie di accesso a distanza che combinano una protezione tramite password con una soluzione di autenticazione a più fattori. Questo è spesso il caso delle VPN. Tuttavia, molte aziende non se la sentono di farsi carico dei relativi costi e si affidano esclusivamente a sistemi protetti da password. In questo ambito, ci si avvale spesso del Remote Desktop Protocol (RDP). Gli hacker individuano con relativa rapidità queste interfacce RDP e molti di loro, a seguito di tentativi con nomi utente e combinazioni di password, sono riusciti a stabilire una sessione di remote-desktop. A partire da questo momento l'hacker ha la possibilità di penetrare ulteriormente nella rete per sottrarre i dati o eseguire attacchi «ransomware».

Phishing

Nel phishing svolge un ruolo di primo piano il fattore «umano», perché il collaboratore assume involontariamente un ruolo attivo nell'attacco informatico. Il phishing è un tipo speciale di Social Engineering, ovvero di manipolazione sociale. Obiettivo del Social Engineering è indurre le persone a compiere azioni che sono dannose per loro stesse. Quando questa manipolazione avviene via e-mail, generalmente si parla di phishing. Attraverso le e-mail di phishing i collaboratori vengono indotti a fornire informazioni confidenziali o a installare software dannosi sul loro computer, ad esempio tramite allegato o link a un sito web. Successivamente gli hacker possono entrare più in profondità nella rete per sottrarre dati o mettere in atto attacchi ransomware.

Trucchi tipici degli hacker

Modelli d' attacco **Porte d' accesso**

Infezione drive-by
In molte aziende le applicazioni vengono aggiornate troppo raramente. Spesso si utilizzano browser con punti deboli noti, ad esempio nei cosiddetti «plugin». In questo caso è sufficiente che un collaboratore visiti un sito web hackerato oppure «maligno»: questo sito identifica il punto debole e si annida nel sistema informatico della vittima. La visita a un sito web sbagliato può quindi essere sufficiente a trasportare software nocivo all'interno dell'azienda.

Sistemi non aggiornati o configurazioni errate
Al giorno d'oggi, praticamente ogni impresa gestisce numerosi sistemi IT che sono collegati direttamente con Internet e quindi possono essere accessibili da tutto il mondo. Questi sistemi sono costituiti dal sistema operativo e solitamente da una serie di applicazioni. Di conseguenza, la maggior parte delle imprese sono oberate dalla necessità di tenere costantemente aggiornati tutti i sistemi, senza contare che praticamente ogni giorno appaiono nuovi aggiornamenti e «patch di sicurezza» dei fornitori di software. Accade così che falle di sicurezza non vengano risolte per mesi o persino per anni. Non appena un hacker identifica queste falle di sicurezza può sfruttarle (ad es. tramite il cosiddetto «exploit») per accedere ai dati o acquisire il controllo dei sistemi.

Parti terze (ad es. fornitori di servici esterni)
Quando si sfruttano «porte di accesso» per azioni a distanza, phishing, drive-by-infection o sistemi non aggiornati si è in presenza di un attacco diretto all'impresa. Ma i criminali informatici possono anche sfruttare i punti deboli di parti terze. Se un'impresa condivide dati sensibili con un fornitore terzo, oppure se acquista servizi software da questo, quest'impresa è soggetta non solo ai propri rischi per la sicurezza, ma anche a quelli del fornitore di servizi

Armatevi e riducete i vostri rischi

Gli otto suggerimenti più importanti Altre informazioni sul tema

Sebbene ogni impresa sia unica, abbiamo preparato per voi una lista con i principali suggerimenti:

1. Analisi del rischio come compito di management: quali sono i miei «gioielli della corona» e come posso proteggerli? In questo ambito rientra anche la gestione professionale delle crisi, con piano d'emergenza per gli attacchi informatici.

2. Istruite i vostri collaboratori a gestire i dati e le e-mail, dal momento che spesso sono proprio loro a rappresentare la porta d'accesso dei malware e quindi anche degli attacchi

3. Verificare annualmente i diritti utente e i cambi di funzione – in questo modo potete impedire che ad esempio degli ex collaboratori accedano alla rete.

4. Utilizzare password intelligenti, che contengano ad esempio caratteri speciali, combinino cifre e lettere, abbiano almeno otto caratteri e nelle quali non compaia il proprio nome. Non utilizzate più volte le stesse password, cambiatele periodicamente e non condividetele con terzi.

5. Assicuratevi che anche gli accessi a distanza siano ben protetti e abbinati a una soluzione di autenticazione a più fattori. È opportuno anche limitare gli accessi esterni dal punto di vista dello spazio e tempo, ad es. solamente da determinati indirizzi IP e in determinati orari (ad es. finestre di manutenzione).

6. Mantenere aggiornato il sistema operativo, poiché gli hacker accedono attraverso i punti deboli nel software. È opportuno anche rimuovere i vecchi sistemi operativi (ad es. Windows XP, Windows 7), perché non ricevono più alcun aggiornamento. Inoltre, è utile creare un inventario di tutti i computer e di tutte le applicazioni dell'azienda, in modo da avere una panoramica di tutti i sistemi IT in uso.

7. Installare programmi antivirus che riconoscano e blocchino i malware e utilizzare un firewall che impedisca gli accessi non consentiti. I programmi andrebbero aggiornati su base quotidiana

8. Eseguite periodicamente backup dei dati, con frequenza giornaliera o anche più spesso, a seconda della loro importanza. Il backup più recente non dovrebbe sovrascrivere quello precedente poiché altrimenti i dati storici potrebbero andar perduti. Banale, ma importante: una copia di back-up dovrebbe essere sempre staccata dalla rete, in modo da non essere sottratta in caso di attacco hacker. Occorre testare regolarmente se il backup dei dati ha funzionato.

Armatevi e riducete i vostri rischi

Desiderate informarvi in modo dettagliato su come ridurre al minimo i rischi informatici per la vostra impresa? Allora vi consigliamo le seguenti informazioni supplementari:

Con la piattaforma digitale «**Zurich Risk Advisor**» potete effettuare un'auto-valutazione dei vostri rischi informatici. La valutazione comprende cinque moduli e vi fornisce concrete proposte di miglioramento. Informatevi sul nostro sito (in inglese) e scaricate l'app: **Link**

Il **Centro nazionale per la cybersicurezza (NCSC)** è il centro di competenza della Confederazione per la sicurezza informatica. L'obiettivo di questa autorità è proteggere la Svizzera dai rischi informatici. Sulla pagina informativa per le imprese, il NCSC mette in guardia dai pericoli attuali e fornisce una panoramica generale sul modo in cui le imprese si possono difendere dai rischi informatici: **Link**

Anche l'associazione mantello dell'economia ICT in Svizzera, **ICT Switzerland**, desidera fornire un supporto alle PMI svizzere per ridurre i rischi informatici ed ha realizzato una guida in proposito: **Link**

Il sistema di sicurezza di Zurich

1 Prevenzione

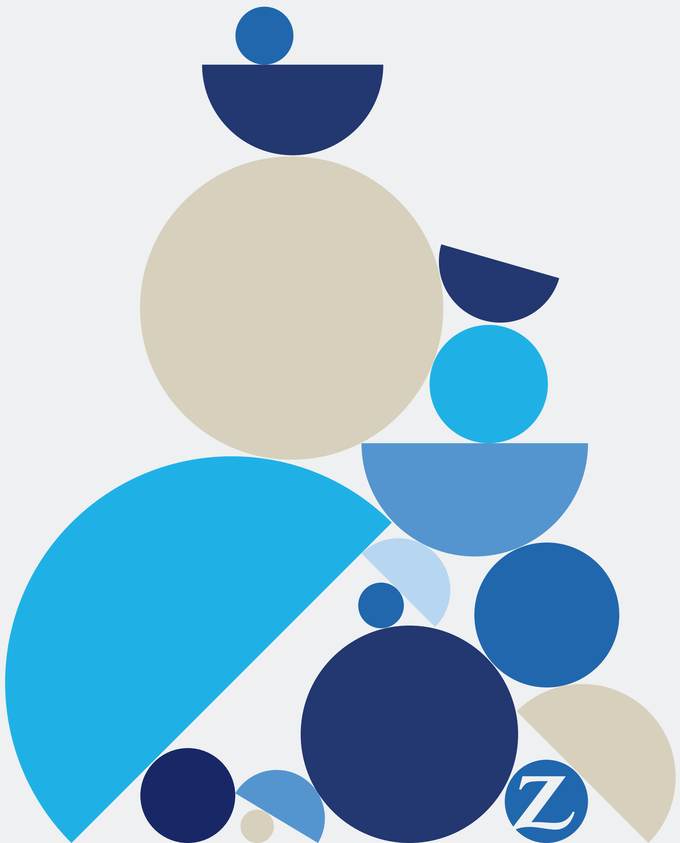
Insieme al nostro partner vi forniamo un supporto per ridurre al minimo i rischi della vostra azienda.

2 Protezione dai rischi finanziari

I nostri moduli di copertura vi offrono la soluzione assicurativa più adatta a voi.

3 Gestione dei sinistri

Nei casi seri, un intervento rapido e adeguato è fondamentale per il successo delle misure.



Il sistema di sicurezza di Zurich

Il sistema di sicurezza di Zurich vi aiuta a comprendere i rischi cui siete esposti e a proteggervi dagli attacchi informatici. Insieme al nostro partner vi forniamo un supporto per ridurre al minimo i rischi della vostra azienda.

Formazione sulla sicurezza informatica: perché i collaboratori non diventino complici

Per quanto riguarda il tema della sicurezza elettronica, l'anello più debole è rappresentato dal fattore umano. In tutti i tipi di aziende, le e-mail non riconosciute degli hacker sono la porta di accesso più frequente per gli attacchi informatici mirati. Proprio in questo ambito interviene Zurich con la sua formazione gratuito sulla sicurezza informatica per clienti Zurich e i loro collaboratori. Il training online è stato sviluppato dalla nostra azienda partner SoSafe, specializzata in e-learning e sicurezza informatica. I cinque moduli di e-learning e la simulazione di phishing intendono sensibilizzare i collaboratori nei confronti dei rischi presenti su Internet e impedire così che diventino dei complici involontari.

Valutazione dei rischi

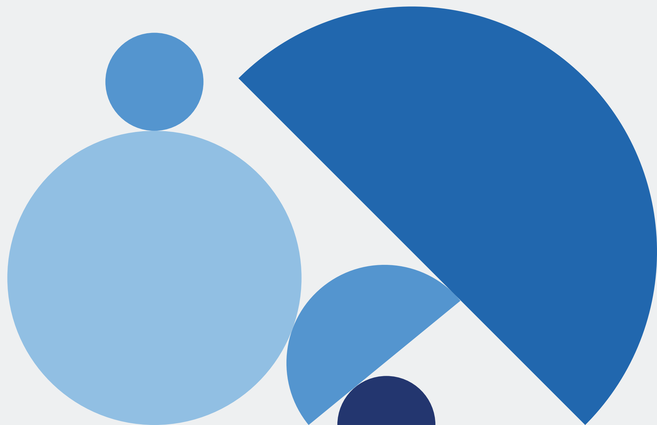
Insieme a Spie ICS, uno dei fornitori leader per la tecnologia dell'informazione e della comunicazione in Svizzera, Zurich ha sviluppato un security check e un security assessment. Le due analisi hanno lo scopo di identificare i vostri rischi nell'ambito della sicurezza informatica, di valutarli e di fornire raccomandazioni attuabili. Le analisi vengono eseguite da esperti di Spie.

Security check (tempo richiesto per voi: un'ora)
L'analisi si svolge in loco presso di voi. Con appositi tool si verificano i punti deboli dei vostri sistemi e delle vostre applicazioni. Vi viene quindi fornito un rapporto che illustra l'urgenza dei punti deboli, incluse le misure di riparazione/riduzione.

Security assessment (tempo richiesto per voi: due ore)
L'analisi completa dei processi di sicurezza e i controlli di affidabilità, integrità e disponibilità di sistemi/applicazioni si svolgono in loco presso di voi.
A tal fine si svolgerà un colloquio strutturato con voi.

Riceverete quindi un rapporto dettagliato con i seguenti contenuti:
– Stato dei controlli di sicurezza
– Punti deboli identificati
– Raccomandazioni per la riduzione dei rischi.

In quanto clienti informatici di Zurich, potrete beneficiare con Spie ICS di condizioni speciali per lo svolgimento di un security check o di un security assessment. I costi vengono calcolati sulla base del numero di postazioni di lavoro con computer: il costo del security check parte da CHF 630 (fino a 10 postazioni di lavoro), quello del security assessment da CHF 1'600 (fino a 10 postazioni di lavoro).



Il sistema di sicurezza di Zurich

I nostri moduli di copertura vi offrono la soluzione assicurativa più adatta a voi

Anche un solido sistema di sicurezza informatica, purtroppo, non garantisce una protezione assoluta dagli attacchi informatici. Nel caso in cui si dovesse verificare un sinistro in questo ambito, Zurich offre la copertura assicurativa ottimale e vi fornisce un supporto per superare le conseguenze.

Selezionate il pacchetto adatto alla vostra impresa:

Basic da CHF 410	Ripristino dei sistemi e dei dati informatici Gestione delle crisi informatiche Responsabilità civile per attacchi informatici Protezione giuridica in ambito informatico
Optimum da CHF 690	+ Interruzione di esercizio per attacco informatico
Premium da CHF 845	+ Cyber-Crime

Il sistema di sicurezza di Zurich

1. Prevenzione **2. Protezione dai rischi finanziari** 3. Gestione dei sinistri

Ripristino dei sistemi e dei dati informatici

- Chiarimenti tecnici e indagini forensi informatiche: Cosa è successo esattamente?
- Ripristino o recupero di dati e informazioni
- Recupero dell'hardware danneggiato (bricking)
- Identificazione dei punti deboli dei software e misure per il miglioramento della sicurezza (betterment)
- Pagamenti di ricatti informatici e spese per la difesa da questi
- Assunzione dei costi in caso di hacking telefonico

Basic Optimum Premium

Gestione delle crisi informatiche

- Verifica degli obblighi di dichiarazione e di notifica
- Notifica alle persone interessate su base volontaria
- Procedure amministrative nonché sanzioni e multe (assicurabili)
- Penalità contrattuali in caso di violazione degli standard PCI DSS
- Call center, monitoraggio delle carte di credito e dell'identità per le persone interessate
- Iniziative benefiche come promozioni e sconti per le persone interessate
- Progettazione ed esecuzione di campagne di relazioni pubbliche in caso di resoconti mediatici negativi

Basic Optimum Premium

Responsabilità civile per attacchi informatici

Risarcimento danni e difesa da pretese ingiustificate relative a:

- Perdita, furto o pubblicazione di dati, a prescindere dal verificarsi di un incidente informatico
- Violazione delle leggi sulla protezione dei dati (incluso GDPR)
- Violazione dei diritti al nome, d'autore e di marchio
- Spese processuali e di difesa

Basic Optimum Premium

Protezione giuridica in ambito informatico

- Consulenza circa le misure giuridiche immediate
- Rivendicazione di pretese di risarcimento
- Difesa in un processo penale in caso di violazione per negligenza di norme sulla protezione dei dati

Basic Optimum Premium

Interruzione di esercizio per attacco informatico e spese supplementari

- A seguito di un incidente informatico o a un uso scorretto
- A seguito di una disposizione amministrativa per la violazione delle norme sulla protezione dei dati
- Copertura della perdita di utili netti nonché delle spese supplementari per il mantenimento dell'attività

Optimum Premium

Cyber-Crime

- Truffa informatica tramite inganno attivo di terzi (ingegneria sociale)
- Furto informatico tramite manipolazione di sistemi informatici da parte di terzi (hackeraggio dell'e-banking)

Premium

Il sistema di sicurezza di Zurich

Nei casi seri, un intervento rapido e adeguato è fondamentale per il successo delle misure.

In caso di sinistro bisogna agire rapidamente. La nostra hotline è raggiungibile quindi 7 giorni su 7 e 24 ore su 24. Durante gli orari di ufficio, i nostri collaboratori specializzati in danni informatici si occupano del vostro caso. Al di fuori degli orari di ufficio, la vostra chiamata viene inoltrata direttamente al nostro partner IT Compass Security.

A seconda della necessità, affidiamo il vostro caso alla gestione da parte di esperti. A questo fine collaboriamo anche con la società di sicurezza IT Compass Security. Grazie alla sua esperienza e perizia, il nostro partner è ottimamente attrezzato per trovare una soluzione rapida e sostenibile al vostro problema informatico. Inoltre, sulla base dell'analisi delle cause vi vengono consigliate delle misure per una protezione informatica costante. In questo modo potrete assicurare alla vostra impresa una protezione globale per il futuro.

Non ci limitiamo a fornirvi un aiuto nei problemi IT, ma disponiamo anche dei partner adatti per questioni giuridiche, che si tratti della verifica dell'obbligo d'informazione, della difesa da pretese di risarcimento danni o della presentazione di denunce. Anche la reputazione della vostra impresa può rapidamente essere messa in discussione. Per questo motivo, in caso di particolare emergenza possiamo procurarvi specialisti che si occupino della comunicazione nei confronti di partner esterni e che vi aiutino così a proteggere la vostra immagine.

Il sistema di sicurezza di Zurich

1. Prevenzione 2. Protezione dai rischi finanziari **3. Gestione dei sinistri**

Processo relativo ai sinistri in ambito informatico: il caso di sinistro è il «momento della verità» – fedeli alla promessa «Siamo al vostro servizio quando avete bisogno di noi».

Stipulazione del contratto

Congratulazioni per aver stipulato la Cyber assicurazione di Zurich. Siamo a sua completa disposizione per qualsiasi domanda e le offriamo un training di sensibilizzazione gratuito per i suoi collaboratori, oltre a una valutazione del rischio informatico quale servizio opzionale.

Evento

Ha constatato delle irregolarità nel suo sistema IT o è stato vittima di un attacco informatico.

Segnalazione

Ci segnali l'evento in tutta semplicità, 24 ore su 24 e 7 giorni su 7, al:

044 629 10 40

zurich.ch/dichiarazione-sinistro

Saremo lieti di chiarire la situazione insieme e di concordare le ulteriori procedure.

Misura

Se necessario, Zurich la metterà in contatto con uno specialista IT che adotterà misure immediate e/o garantirà la completa risoluzione del guasto. In alternativa, può affidare la risoluzione del problema al suo partner IT.

Procedura

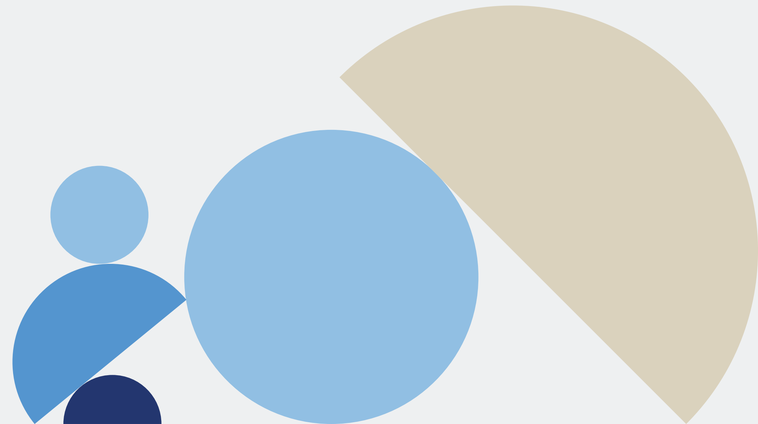
Zurich esamina il rapporto d'analisi dello specialista IT. Zurich verifica l'indennità.

Liquidazione

Discutiamo con lei la liquidazione del sinistro. Unitamente alla comunicazione conclusiva riceverà un riassunto dei costi e la conferma del pagamento del sinistro.

Post-sinistro

Come servizio opzionale, può ricevere consigli sulla prevenzione da parte dei nostri specialisti IT.



Esempi di sinistri: studio medico (1/2)

Furto di dati in uno studio medico a seguito di attacco hacker al fornitore di servizi IT

1 Situazione iniziale

Lo **studio medico** Arzt-Muster Sagl è un centro associato formato da più pediatri

Fatturato annuo: CHF 1’500’000
Numero di collaboratori: 6

L’infrastruttura IT (incluso il sistema di gestione dei pazienti) è messa a disposizione da un fornitore di servizi IT. I collaboratori utilizzano notebook che sono collegati con il server. I dati vengono memorizzati direttamente sul server.

2 Descrizione del sinistro

A seguito di un attacco hacker al fornitore di servizi IT dello studio medico Arzt-Muster Sagl, soggetti non autorizzati ottengono l’accesso ai dati dei pazienti. I medici non sono sicuri di quali siano i dati interessati dall’attacco e di che tipo di danni possa provocare l’hacker.

3 Come aiuta Zurich

Pacchetto Basic

Gestione del sinistro

- Zurich chiede al contraente se il suo fornitore di servizi IT ha bisogno di aiuto per rimuovere il danno. Il fornitore sta già lavorando all’accertamento dell evento e al ripristino del funzionamento della struttura IT. Tuttavia, ben presto si accerta che per la valutazione della portata dei danni è necessario avvalersi del supporto di esperti. Zurich organizza rapidamente il supporto necessario alfine di chiarire quali dati dei pazienti sono stati interessati dall’attacco informatico.
- Inoltre, attraverso il proprio partner Zurich offre ai medici una consulenza giuridica competente in merito all’obbligo d’informazione e alla responsabilità civile. Proprio in considerazione della prevista revisione della Legge sulla protezione dei dati e degli elevati rischi legali connessi a seguito di una regolamentazione più severa, diventa ancora più importante avvalersi di una perizia specializzata.
- In quanto servizio previsto della gestione dei sinistri, gli esperti del partner di Zurich di relazioni pubbliche forniscono assistenza allo studio medico nel fornire informazioni adeguate a tutte le persone coinvolte.

Esempi di sinistri: studio medico (2/2)

Protezione dai rischi finanziari

- Modulo Ripristino dei sistemi e dei dati informatici
  Il partner forense IT di Zurich analizza l'entità dei danni e verifica quali dati e quali pazienti ne sono coinvolti. Sulla base dell'analisi, l'esperto IT è in grado di valutare quali sono i danni che l'hacker può provocare utilizzando i dati sottratti. Nel caso in cui i dati non fossero sufficientemente protetti, si può presumere che l'hacker cerchi di trarne profitto nella darknet. Se i dati e i sistemi dello studio medico sono stati corrotti, Zurich si fa carico dei costi per il ripristino dei dati e dell'infrastruttura IT.

- Modulo Protezione giuridica in ambito informatico
  Bisogna verificare in che misura i pazienti coinvolti e le autorità debbano essere informati del furto dei dati. L'analisi iniziale è compresa nell'assicurazione della protezione giuridica.

- Modulo Responsabilità civile in ambito informatico
  Qualora dall'analisi iniziale dovesse emergere che non è avvenuta alcuna violazione legale, Zurich fornirà la difesa da pretese di responsabilità civile ingiustificate. Nel caso in cui i dati personali non fossero sufficientemente protetti, sussiste il rischio che vengano avanzate rivendicazioni legittime di responsabilità. In tal caso Zurich fornisce un risarcimento danni.

- Modulo Gestione delle crisi informatiche
  Sulla base delle conoscenze acquisite dall'analisi del sinistro si sviluppa un'adeguata strategia di comunicazione. I costi per la comunicazione sono a carico di Zurich. Qualora dall'analisi iniziale dovesse emergere che è avvenuta una violazione legale, sono assicurati anche i costi relativi alle comunicazioni nei confronti delle autorità.

- Panoramica dei costi assicurati in questo esempio
  Costi per attività forense IT e per le consulenze in materia di comunicazione; altri eventuali costi per consulenza legale/controversia giuridica a seconda della situazione (con riserva di deduzione di franchigia a seconda dell'accordo)

Esempi di sinistri: costruttore (1/2)

Arresto della produzione di un costruttore di parti metalliche a seguito di un accesso in remoto

1 Situazione iniziale

Il **costruttore** Pezzi di ferro SA offre una gamma universale di parti metalliche con rapidi tempi di consegna.

Fatturato annuo: CHF 3’000’000
Numero di collaboratori: 15

L’intera **infrastruttura IT** si trova sull’area dell'azienda; oltre alla rete aziendale amministrativa, l’impresa possiede anche una rete per le macchine di produzione. Queste sono collegate in Internet con possibilità di accesso a distanza, in modo che il costruttore possa garantire in qualsiasi momento la loro manutenzione.

2 Descrizione del sinistro

Domenica, utilizzando una password rubata, un hacker è riuscito ad entrare nella rete interna dell’azienda, bloccando l’intera infrastruttura IT e causando così l’arresto di tutte le macchine produttive. Di conseguenza, per cinque giorni l’azienda non ha più la possibilità di produrre parti in metallo.
Mentre il locale fornitore di servizi IT cerca, in collaborazione con il costruttore di macchine, di eliminare il virus dalla rete e riavviare la produzione, l’imprenditore riceve una telefonata da un importante cliente. Questi desidera effettuare un ordine urgente per un volume di CHF 80'000 e data di completamento entro 7 giorni. Dal momento che l’ordine non può essere differito, a causa dell’attacco informatico l’imprenditore è costretto a rifiutare. Inoltre, deve riuscire a portare a termine entro i prossimi 10 giorni un ordine già esistente. Per garantirlo, tutti i collaboratori della produzione devono svolgere lavori straordinari nel fine settimana.

Dal momento che il fornitore di servizi IT dell’azienda non dispone delle competenze necessarie per l’analisi e la rimozione dei guasti, c’è bisogno di un supporto esterno. L’imprenditore chiede quindi immediatamente aiuto a Zurich.

3 Come aiuta Zurich

Pacchetto Optimum

Gestione dei sinistri
La hotline sinistri per danni informatici è raggiungibile 24/7 e il costruttore può così denunciare il danno a Zurich già domenica sera. Negli orari di ufficio, i danni degli incidenti di natura informatica sono gestiti da collaboratori specializzati. Al di fuori degli orari di ufficio, la chiamata viene inoltrata direttamente al nostro partner IT, che quindi si occupa immediatamente della soluzione del problema. Dopo la chiamata, il nostro partner si assicura anche che un team di Incident Response sia presente sul posto presso il cliente e si occupi della soluzione del problema.

Esempi di sinistri: costruttore (2/2)

Protezione dai rischi finanziari

- Modulo Ripristino dei sistemi e dei dati informatici
  l'incidente informatico causa CHF 4'000 di costi per il fornitore di servizi IT locale. Altri CHF 7'000 sono dovuti per i lavori di manutenzione del costruttore di macchine a seguito dell'attacco informatico. I costi per il rapido intervento del team di Incident Response alfine di ripristinare l'infrastruttura IT e rimuovere i punti deboli ammontano a CHF 13'000.

- Modulo Gestione interruzione di esercizio per attacco informatico
  Il software nocivo introdotto nella rete aziendale blocca l'accesso alle macchine di produzione per cinque giorni. A causa dell'ordine che non è stato possibile accettare, il fatturato perso ammonta a CHF 60'000 (CHF 80'000 per l'ordine meno CHF 20'000 per i costi risparmiati (ad es. materie prime, elettricità, ecc.)). La copertura comprende anche le spese aggiuntive per il secondo ordine che si è potuto svolgere solo grazie al lavoro aggiuntivo nel fine settimana. Ulteriori CHF 5'000 sono stati pagati per il personale addetto alla produzione nei turni speciali.

- Panoramica dei costi assicurati in questo esempio
  CHF 89'000 (con riserva di deduzione di franchigia in base all'accordo)

Esempi di sinistri: società fiduciaria (1/2)

Diebstahl von Kundenkonten einer Treuhandfirma durch eine Phishing-Attacke

1 Situazione iniziale

La **società fiduciaria** Martino Torta SA effettua pagamenti su incarico dei propri clienti.

Fatturato annuo: CHF 6’500’000
Numero di collaboratori: 22

L’**infrastruttura IT** è messa a disposizione da un fornitore di servizi IT. I collaboratori utilizzano notebook che si collegano con il server. I dati vengono memorizzati direttamente sul server.

2 Descrizione del sinistro

Un collaboratore cade vittima di un attacco phishing. Riceve una candidatura apparentemente spontanea e clicca sull’allegato, il presunto documento di candidatura. In tal modo, installa inconsapevolmente un virus sul terminale. Attraverso questo malware, quando i collaboratori effettuano il login nel portale e-banking l’hacker può prendere il controllo e dirottare i fondi dai conti bancari dei clienti.

3 Come aiuta Zurich

Pacchetto Premium

Gestione dei sinistri
Non appena la società fiduciaria denuncia il sinistro a Zurich, gli specialisti informatici Zurich prendono immediatamente contatto con il fornitore di servizi IT dell’azienda. Inoltre, forniscono un supporto alla società fiduciaria nelle comunicazioni con le autorità. Il fornitore di servizi IT riesce a riprendere il controllo della situazione in modo relativamente rapido e nel giro di tre giorni lavorativi il malware dannoso viene eliminato dai sistemi. Per garantire che l’hacker non possa più accedere ai sistemi, Zurich mette a disposizione gli esperti forensi IT dell’azienda partner di Zurich, che analizzano tutti i sistemi per individuare possibili tracce dell’attacco. Dall’analisi emerge che l’hacker non dispone di altri punti di accesso e che non sono stati rubati dati della clientela.

Esempi di sinistri: società fiduciaria (2/2)

Protezione dai rischi finanziari

- Modulo Ripristino dei sistemi e dei dati informatici
  i costi per la pulizia dei sistemi e la rimozione dei punti deboli ammontano a CHF 12'000 (costi per il fornitore di servizi IT e per gli esperti forensi IT).

- Modulo Gestione delle crisi informatiche
  Zurich e i propri partner forniscono un supporto al cliente nel gestire le comunicazioni con le autorità.

- Modulo Cyber-Crime
  ai clienti della società fiduciaria sono stati complessivamente rubati CHF 130’000 da un conto gestito dall’assicurato. Il responsabile della fiduciaria tira un sospiro di sollievo quando constata che il danno non è superiore alla somma d’ assicurazione.

- Panoramica dei costi assicurati in questo esempio
  CHF 142'000 (con riserva di deduzione di franchigia in base all’accordo)

Zurich Cyber assicurazione

Contatto e vantaggi

La digitalizzazione offre molte opportunità di crescita alle imprese. Zurich vi mette nella condizione ideale per sfruttare questo potenziale, grazie a misure preventive, un'assicurazione completa dei rischi finanziari e una competente gestione dei sinistri.

La digitalizzazione offre molte opportunità di crescita alle imprese. Zurich vi mette nella condizione ideale per sfruttare questo potenziale, grazie a misure preventive, un'assicurazione completa dei rischi finanziari e una competente gestione dei sinistri.

Per ulteriori informazioni su Zurich Cyber assicurazione, visitate il nostro sito web. Saremo lieti di fornirvi una consulenza individuale e personalizzata. Rivolgetevi all'agenzia Zurich più vicina, telefonateci al numero gratuito 0800 80 80 80 oppure contattate direttamente il vostro broker/intermediario.

Vantaggi di Zurich Cyber assicurazione

- Vi aiutiamo a proteggere la vostra azienda dai rischi informatici con una formazione sulla sicurezza informatica gratuito per i vostri collaboratori e una valutazione dettagliata dei rischi da parte della nostra azienda partner Spie, con condizioni privilegiate per i clienti Zurich.
- Le coperture sono descritte in modo semplice e chiaro. In questo modo potete sempre sapere cosa è assicurato e cosa no.
- Le ampie coperture complementari tengono in considerazione sia le esigenze specifiche del vostro settore, sia i nuovi rischi.
- Grazie ai nostri specialisti Zurich e alla nostra rete professionale di partner, in caso di sinistro Zurich può fornirvi un'assistenza competente, lasciandovi comunque la libertà di scegliere il fornitore di servizi.
- Non ci limitiamo a occuparci della riparazione del danno, ma ricerchiamo le cause e vi aiutiamo ad eliminare i punti deboli anche per il futuro.
- L'offerta concepita è stata pensata per piccole e per medie imprese.