Information Security Society Switzerland

e il vostro computer è al sicuro.

Maggiore sicurezza dell'informazione per le piccole e medie imprese (PMI)

Il Programma in 10 punti ampliato offre una protezione maggiore.

Collana PMI «Dalla pratica – per la pratica»

Concezione e testo
Gruppo di lavoro PMI + sicurezza dell'informazione dell'associazione InfoSurance:
Ueli Brügger, IBM, Zurigo
Christof Egli, Ernst Basler + Partner, Zurigo (responsabile del gruppo di lavoro)
Hanspeter Feuz, IT Projects, Thun
Tiziana Giorgetti, Symantec Switzerland AG, Bassersdorf
René Hanselmann, Microsoft GmbH, Wallisellen
Peter Neuhaus, Fondazione PMI Svizzera, Berna
Il gruppo di lavoro è stato sostenuto da:
Jürg Altenburger, IBM, Zurigo
Chris Baur, Trivadis AG, Zurigo
Diego Boscardin, Symantec Switzerland AG, Bassersdorf
Herbert Brun, UPAQ Ltd., Küsnacht
Roger Halbheer, Microsoft GmbH, Wallisellen
Andrea Müller, Microsoft GmbH, Wallisellen
Peter Kunz, Omnisec, Dällikon
Anton Lagger, Ufficio federale per l'approvvigionamento economico del Paese, Berna
Marc Vallotton, InfoGuard AG, Zugo
Christian Weber, Segreteria di Stato dell'economia SECO, Berna
Carlos Rieder, Scuola universitaria di economia di Lucerna
Niklaus Schild, Trivadis AG, Zurigo
Wolfgang Sidler, SIDLER Information Security GmbH, Hünenberg
Concezione grafica, layout
Künzli Communication AG, Lucerna
Stampa
Gisler Druck AG, Altdorf

Gentile amministratrice di una PMI,
Egregio amministratore di una PMI,

Nelle statistiche mondiali la Svizzera compare come una delle nazioni con il maggior numero di utilizzatori di tecnologie dell'informazione e della comunicazione. Nessuno spende di più del cittadino medio svizzero quando si tratta di tecnologie dell'informazione (IT).

Non si può fare a meno dell'IT – nemmeno voi in qualità di amministratori di una piccola o media impresa svizzera. Le PMI sono innegabilmente i pilastri dell'economia svizzera. Godono di una fama eccezionale e i loro prodotti e servizi si basano su qualità, flessibilità e potenziale innovativo.

L'associazione InfoSurance studia da anni i rischi che corrono le PMI nell'uso dell'IT. Per sostenere le imprese nell'introduzione di una protezione adeguata, nel 2005 InfoSurance ha pubblicato l'opuscolo **Programma in 10 punti per una protezione di base efficace nell'IT**.

Ora l'associazione InfoSurance ha integrato il programma con altri dieci punti che si rivolgono in particolare a quelle PMI che hanno un bisogno maggiore di disponibilità e riservatezza dei sistemi e dei dati.

Il **Programma in 10 punti ampliato** si contraddistingue anch'esso per la sua semplicità, e vi permette di attuare le misure descritte al suo interno senza incorrere in costi elevati. Se non disponete di competenze specialistiche, vi raccomandiamo di farvi aiutare da uno specialista esterno.

Una buona gestione imprenditoriale comprende anche le attività di gestione dei rischi. Per questo motivo il legislatore richiede, dal 1° gennaio 2008, l'indicazione di come vengono gestiti i rischi e l'attestazione dell'esistenza di un sistema di controllo interno (SCI). Il presente opuscolo vi offre un valido supporto in materia di IT.

Vi invitiamo a leggere il Programma in 10 punti ampliato con la stessa attenzione che avete dedicato al primo programma.

Auguro a voi e alla vostra impresa pieno successo nel miglioramento della sicurezza.

Consigliere nazionale Edi Engelberger

Presidente dell'Unione svizzera delle arti e mestieri

Il Programma in 10 punti ampliato in sintesi

10 misure per una protezione di base efficace

Punto 1 Redigete un quaderno degli obblighi per i responsabili IT!
Punto 2 Eseguite backup regolari dei vostri dati!
Punto 3 Aggiornate sempre il vostro programma antivirus!
Punto 4 Proteggete il vostro accesso a Internet con un firewall!
Punto 5 Aggiornate il vostro software periodicamente!
Punto 6 Utilizzate password sicure!
Punto 7 Proteggete i vostri dispositivi mobili!
Punto 8 Fate conoscere le vostre linee guida per l'utente IT!
Punto 9 Proteggete l'ambiente della vostra infrastruttura IT!
Punto 10 Tenete in ordine i documenti e i supporti dati!

5 ulteriori misure per una maggiore riservatezza

Punto 11 Rispettate le disposizioni!
Punto 12 Disciplinate la protezione dell'accesso ai dati!
Punto 13 Cifrate i supporti dati mobili e le trasmissioni!
Punto 14 Trattate con riservatezza anche i dati non elettronici!
Punto 15 Sensibilizzate i vostri collaboratori!

5 ulteriori misure per una maggiore disponibilità

Punto 16 Controllate i vostri sistemi!
Punto 17 Garantite un approvvigionamento elettrico senza interruzioni!
Punto 18 Garantite la ridondanza degli elementi importanti!
Punto 19 Predisponete un piano d'emergenza!
Punto 20 Distribuite il know-how!

Redigete un quaderno degli obblighi per i responsabili IT!

La sicurezza informatica dipende in pari misura da fattori tecnici, organizzativi e umani! Accanto alle soluzioni di sicurezza tecniche e a collaboratori motivati anche il Comitato direttivo deve contribuire ad attuare un'efficace protezione di base.

In ogni impresa deve esserci un responsabile EED o • IT con il rispettivo sostituto. Le competenze necessarie si possono acquisire attraverso appositi corsi di formazione. Spesso le piccole imprese collaborano anche con specialisti esterni, i costi dei quali sono di molto inferiori rispetto alle conseguenze di una perdita di dati o di una violazione della Legge sulla protezione dei dati.

Il Comitato direttivo delega per iscritto al respon• sabile IT i compiti di sicurezza e li elenca all'interno di un quaderno degli obblighi (vedi sotto).

Il Comitato direttivo controlla che il responsabile IT • esegua correttamente i suoi compiti.

A tutti i collaboratori che lavorano a un computer• vengono fornite delle linee guida per l'utente all'interno delle quali sono descritte le operazioni permesse e vietate (vedi punto 8).

Stabilite un referente per tutte le questioni attinenti• alla sicurezza, per es. la perdita di un notebook, un'infezione da virus, ecc.

Consigli e suggerimenti

Eseguite backup regolari dei dati memorizzati su • server, postazioni di lavoro, notebook, laptop e altri dispositivi mobili (vedi punto 2).

Mantenete aggiornati sistemi operativi, programmi • antivirus, firewall e ogni altro software (vedi punti 3, 4 e 5).

Modificate subito le password predefinite per di• spositivi, sistemi operativi e applicazioni.

Tenete un elenco di tutti i computer presenti • nell'impresa, compresi i relativi programmi installati e gli aggiornamenti software eseguiti (vedi punto 5).

Stabilite i diritti di accesso: quali programmi pos• sono eseguire i collaboratori? A quali dati hanno accesso?

Tenete un elenco di tutte le persone che accedono• alla rete aziendale dall'esterno, eventualmente con la durata precisa della concessione dei diritti. Assicuratevi che anche i loro programmi di protezione siano aggiornati.

Assicuratevi che le disposizioni sulla protezione • dei dati vengano rispettate, per es. con programmi di protezione aggiornati e password sicure (vedi punti 3, 4 e 6).

Verificate regolarmente che le linee guida per • l'utente vengano rispettate.

Considerate le attività di sicurezza come un • progetto:volete ottenere un certo risultato con le risorse disponibili entro una data scadenza.

La sicurezza è un processo: verificate periodica• mente lo stato della sicurezza e se necessario apportate dei miglioramenti (orientatevi al «ciclo di Deming»: Plan – Do – Check – Act).

Eseguite backup regolari dei vostri dati!

Le perdite di dati si verificano in tanti modi diversi: i dati vengono sovrascritti per sbaglio, un difetto rende illeggibili le informazioni di un disco rigido oppure un incendio o un allagamento distruggono i vostri supporti di archiviazione. Queste perdite si possono evitare creando copie di sicurezza (backup) periodiche.

- Fondamentalmente bisogna effettuare un backup di tutti i dati importanti per l'attività produttiva. È consigliabile salvare anche le configurazioni software.
- La frequenza del backup dei dati dipende dall'attività e dalle dimensioni della vostra impresa. Ogni PMI dovrebbe creare un backup dei dati almeno una volta a settimana.
- L'esecuzione di un backup giornaliero rende l'archiviazione dei vostri dati conforme al diritto delle obbligazioni e all'«Ordinanza sulla tenuta e la conservazione dei libri di commercio» (Olc) (vedi sotto).
- Definite per iscritto a chi è affidata la responsabilità del backup dei dati e redigete un elenco di controllo per verificare la correttezza dell'operazione.
- Salvate sempre i dati su supporti mobili (unità a nastro, supporti dati intercambiabili).
- È utile effettuare delle copie dei dati importanti disponibili soltanto in formato cartaceo (per es. contratti, documenti ufficiali) e conservare tali copie fuori sede.
- Ricordate che lo stato patrimoniale, il conto economico, i libri di commercio, gli inventari, i giustificativi contabili e la corrispondenza aziendale devono essere conservati per 10 anni.

Consigli e suggerimenti

- Dal lunedì al giovedì create ogni giorno un backup giornaliero su un supporto di memorizzazione diverso.La settimana seguente sovrascriverete il backup della rispettiva giornata. Conservate le copie giornaliere al di fuori del locale server.
- Ogni venerdì create un backup settimanale su un supporto di memorizzazione separato e conservatelo al di fuori della sede dell'attività. Il backup settimanale andrà sovrascritto dopo un mese.
- Alla fine del mese preparate un backup mensile. Il backup mensile non andrà sovrascritto, e lo si conserverà al di fuori della sede dell'impresa.
- A fine anno create il backup annuale. Il backup annuale non andrà sovrascritto, e anche questo lo si conserverà al di fuori della sede dell'impresa.
- Verificate periodicamente se è possibile ripristinare i dati dai supporti di backup. Qualsiasi backup, infatti, è inutile se i dati non sono stati trasferiti correttamente sul supporto.

Aggiornate sempre il vostro programma antivirus!

Programmi dannosi come virus e worm possono paralizzare la vostra infrastruttura informatica e quindi mettere a rischio la sussistenza economica della vostra impresa.

I virus informatici sono in grado di modificare, • manipolare o persino distruggere del tutto dati e programmi. Queste applicazioni dannose si trasmettono tramite allegati e-mail (attachment), Instant Messenger, ecc. In Internet i virus sono spesso mascherati da programmi gratuiti utili o di intrattenimento e si attivano con un semplice clic del mouse.

I sistemi informatici con una protezione insuffi• ciente vengono spesso utilizzati abusivamente per diffondere i virus o per sferrare attacchi mirati contro terze imprese. Se un amministratore aziendale adotta precauzioni insufficienti per proteggere i suoi sistemi informatici si espone ad accuse di negligenza e a un eventuale procedimento penale.

Per proteggersi dai virus e worm noti si usa un • programma antivirus, che è in grado di identificare gli intrusi e renderli innocui. Questi programmi possono essere acquistati nei negozi di informatica oppure scaricati gratuitamente da Internet.

Dato che i pirati informatici programmano sempre • nuovi virus, il programma antivirus va aggiornato costantemente. A seconda del prodotto utilizzato il programma cerca autonomamente la disponibilità di aggiornamenti sul sito del produttore. Chiedete al rivenditore se anche il vostro programma prevede questa funzione. L'aggiornamento andrebbe comunque eseguito quotidianamente.

Consigli e suggerimenti

Installate un programma antivirus su tutti i server, • le postazioni di lavoro (client) e sui vostri notebook ed eseguitene l'aggiornamento periodicamente, almeno una volta al giorno.

Vietate esplicitamente la disattivazione temporanea • o completa del programma antivirus.

Invitate i collaboratori a segnalare immediatamente • al responsabile IT gli avvisi relativi ai virus.

Almeno una volta a settimana eseguite una «scan• sione antivirus» completa dei dischi rigidi. In questo modo vengono scoperti ed eliminati i virus che fino a quel momento non si conoscevano.

Vietate esplicitamente l'esecuzione di test che com• portano l'uso di virus.

Nelle reti più ampie aggiornate i programmi antivi• rus centralmente e in modo automatico.

Proteggete il vostro accesso a Internet con un firewall!

Nella vostra azienda ci sono delle porte tagliafuoco? Sì? Allora farete sicuramente attenzione anche a farle chiudere sempre. Nel mondo di Internet e delle trasmissioni elettroniche di dati questo compito di sicurezza è svolto dal firewall.

Senza un firewall le persone non autorizzate • possono danneggiare i vostri sistemi informatici, per esempio eseguendo operazioni senza che ve ne accorgiate o sfruttando i vostri PC per lanciare attacchi illegali contro terzi. Inoltre possono accedere ai dati aziendali, compresi quelli eventualmente assoggettati alla Legge sulla protezione dei dati.

Per le reti aziendali più ampie si raccomanda l'uso • di un firewall a sé stante (un dispositivo speciale), per i PC singoli e i dispositivi mobili (notebook) un firewall integrato (nel sistema stesso).

In commercio sono disponibili prodotti che offrono • contemporaneamente la protezione di un firewall e un antivirus. Questo tipo di prodotti combinati è particolarmente adatto alle aziende più piccole.

Alcuni sistemi operativi dispongono di un firewall • integrato. Sfruttate sempre questa possibilità e attivatelo.

Se all'interno della vostra azienda utilizzate una • wireless LAN per i vostri computer, assicuratevi che questi funzionino correttamente e in modo sicuro. Se utilizzati scorrettamente, i dispositivi wireless LAN possono vanificare l'intera protezione del firewall.

Tutti i punti di accesso alla rete devono essere • protetti con un firewall. Tutte le connessioni tra fornitori, clienti, collaboratori interni e in outsourcing (anche con accesso remoto) e la vostra rete devono essere controllate tramite firewall.

Consigli e suggerimenti

Installate un firewall e aggiornatelo regolarmente.•

Fate passare tutto il traffico Internet attraverso il • firewall. Non consentite altri accessi a Internet (per es. via modem).

Non impiegate laptop e dispositivi wireless LAN pri• vati all'interno dell'azienda senza il consenso scritto del responsabile IT.

Proteggete la configurazione del vostro firewall con • una password sicura.

Eseguite un backup periodico della configurazione • del firewall centrale.

Aggiornate il vostro software periodicamente!

Nella vostra auto tenete sempre sotto controllo il livello dell'olio e la pressione dei pneumatici? Speriamo di sì. Così come assicurate una manutenzione regolare della vostra auto, anche i programmi informatici di un'impresa vanno curati e mantenuti sempre aggiornati.

Il software attuale contiene spesso milioni di righe • di codice, ed è inevitabile che ci siano degli errori, malgrado tutti i controlli eseguiti. Per i produttori è pressoché impossibile testare le applicazioni in ogni ambiente e configurazione immaginabile. Per questo mettono a disposizione a intervalli regolari delle cosiddette «patch», una sorta di «toppe per il software» che risolvono gli errori conosciuti.

Se non aggiornate il vostro software o lo fate solo • raramente, i malintenzionati possono sfruttare gli errori noti per manipolare i vostri dati o utilizzare la vostra infrastruttura per i loro fini.

Spesso i sistemi operativi e le applicazioni sono in • grado di aggiornarsi automaticamente via Internet. Una guida su queste funzioni si trova sui siti Web dei produttori di software e nei rispettivi manuali.

Riducete al minimo i vostri «punti deboli» installan• do soltanto il software effettivamente necessario e disattivando i servizi, le autorizzazioni di rete e i protocolli superflui. Quello che non c'è non può essere sfruttato per fini illeciti e non occorre preoccuparsi della relativa manutenzione!

Se scoprite voi stessi dei punti deboli o se il soft• ware si comporta in modo inaspettato, informate il vostro produttore software.

Consigli e suggerimenti

Installate le ultime «patch» per i sistemi operativi e • le applicazioni.

Installate il prima possibile gli «aggiornamenti di • sicurezza» disponibili.

Installate soltanto gli aggiornamenti per la versione • del software che avete in uso.

Installate le «patch» su tutti i computer, vale a dire • anche sui notebook e sui dispositivi dei collaboratori esterni!

Tenete un elenco di quali «update» sono stati instal• lati su quali dispositivi.

Gli ultimi «update» per i prodotti Microsoft sono disponibili qui: www.windowsupdate.com.

Utilizzate password sicure!

Se si conosce il nome utente e la password di un utente è possibile accedere a un sistema e assumere la sua identità (informatica) con tutte le rispettive autorizzazioni di accesso! Il furto di una password può quindi permettere alle persone non autorizzate di accedere senza grande fatica a informazioni aziendali riservate. Annullate la possibilità di un furto di identità nella vostra azienda.

- Le password predefinite per dispositivi, sistemi operativi e applicazioni devono essere modificate immediatamente dal responsabile IT (vedi punto 1).
- Esortate i vostri collaboratori a utilizzare soltanto password sicure e a cambiarle periodicamente. Fate notare a tutti che ciascuno è responsabile delle azioni compiute con il proprio nome utente.
- Le password sicure sono lunghe almeno 8 caratteri e contengono lettere maiuscole e minuscole, cifre e caratteri speciali.

  Ecco come creare una password sicura:

  Esempio 1: dalla semplice parola «Estate» potete ottenere la password sicura «Es$Tate04» inserendo alla terza posizione il carattere «$», proseguendo con una lettera maiuscola e aggiungendo alla fine le cifre «04» come il mese di aprile.

  Esempio 2: dalla frase «Quest'estate siamo andati in quattro a Parigi!» potete ottenere la password sicura «Qesai4aP!» riprendendo in sequenza le iniziali, le cifre e il punto esclamativo. Una frase dotata di senso compiuto si ricorda più facilmente di una password criptica!

Consigli e suggerimenti

- Non utilizzate come password parole che si trovano nei dizionari.
- Non utilizzate password contenenti nomi, numeri AVS e di passaporto o date di nascita propri o dei familiari.
- Verificate la qualità di una password con un appo sito sistema di verifica.
- Cambiate password almeno una volta ogni due mesi. La soluzione ideale sarebbe impostare il sistema affinché richieda obbligatoriamente la modifica della password.
- Non mettete mai le password per iscritto a meno che non conserviate questi appunti in un luogo sicuro, per es. in cassaforte. Molte password si trovano scritte su fogli di carta a meno di un metro di distanza dal computer.
- Non comunicate mai la vostra password a terzi. È possibile lavorare come sostituti anche senza conoscere la password altrui. Se vi rendete contoche qualcun altro conosce la vostra password, cambiatela immediatamente.

All'indirizzo https://passwortcheck.datenschutz.ch è disponibile un sistema per verificare la qualità della vostra password.

Proteggete i vostri dispositivi mobili!

I telefonini, i palmari e i notebook con connessione wireless LAN sono indubbiamente pratici e versatili. Se vengono usati scorrettamente, però, sono un rischio per la sicurezza. Chi ha la necessità di memorizzare dati sensibili sui dispositivi mobili per motivi di lavoro, deve adottare delle precauzioni speciali.

Tutti i dispositivi mobili vanno protetti con una • password sicura (vedi punto 6). Se il dispositivo viene perso o rubato, infatti, per una persona non autorizzata sarebbe un gioco da ragazzi accedere ai vostri dati aziendali.

Sui dispositivi mobili andrebbero salvati esclusiva• mente i dati effettivamente necessari. Effettuatene un backup periodico (vedi punto 2).

I dati aziendali più delicati salvati sui notebook • devono essere crittografati, in modo da impedire che finiscano nelle mani di persone non autorizzate in caso di perdita o furto. Sono disponibili in commercio e si possono scaricare da Internet buoni programmi di crittografia (vedi sotto).

Anche sui dispositivi mobili occorre eseguire perio• dicamente un controllo antivirus, dato che vengono sincronizzati con i vostri altri computer attraverso le funzioni di e-mail, per esempio.

Approfittando di un dispositivo dotato di connes• sione wireless LAN configurato scorrettamente un hacker potrebbe introdursi nella vostra rete aziendale nel giro di pochi minuti e da distanze di più di un chilometro! L'uso di punti di accesso (hotspot) esterni e pubblici deve essere disciplinato in maniera speciale.

Attivate la connettività Bluetooth dei vostri di• spositivi (telefonino, notebook, computer palmare) solo all'occorrenza e in modalità non riconoscibile, altrimenti potrebbero rispondere a vostra insaputa alle richieste di dispositivi sconosciuti (in un'area anche di 100 metri).

Consigli e suggerimenti

Modificate il nome stabilito dal produttore per la • vostra wireless LAN (identificatore del set di servizi – SSID). Il nuovo identificatore non deve in nessun caso contenere il nome della vostra azienda.

Disattivate la trasmissione dell'SSID affinché il vostro • punto d'accesso non sia visibile a terzi.

Attivate la cifratura della trasmissione dati wireless • (WPA2, Wi-Fi Protected Access 2). Modificate la password predefinita del vostro punto d'accesso.

Impostate il filtro per gli indirizzi MAC, di modo che • soltanto i dispositivi noti possano comunicare con il punto d'accesso.

Trasmettete i dati altamente riservati soltanto me• diante connessioni protette anche con una Virtual Private Network (VPN).

Per la crittografia potete usare il prodotto Pretty • Good Privacy (PGP). Il programma PGP per usi commerciali si trova sul sito Web ufficiale http://www.pgp.com/de/index.html.

Per usare la versione standard e gratuita OpenPGP • visitate il sito http://www.gnupg.org/index.it.html.

Fate conoscere le vostre linee guida per l'utente IT!

Senza delle linee guida per l'utente IT vincolanti e comprensibili i vostri collaboratori non possono sapere quali comportamenti sono permessi e quali sono vietati. Le regole vengono prese sul serio solo se sono rispettate anche dai superiori. Tenete un comportamento esemplare in tutte le questioni legate alla sicurezza.

Definite delle linee guida per l'utente IT scritte e • fatele firmare ai collaboratori.
Portate spesso e in modi diversi l'attenzione • dei collaboratori sulla sicurezza all'interno dell'impresa.
Una o due volte l'anno attuate delle iniziative • di sensibilizzazione, anche con mezzi semplici: per es. con un'e-mail a tutti i collaboratori, una circolare nella posta interna, poster in mensa, articoli nel giornale aziendale, ecc.
Organizzate un corso di formazione di base per • tutti i collaboratori (per es. basandovi su questo opuscolo). I principali obiettivi d'apprendimento sono:
– Utilità della sicurezza informatica
– Creazione di password sicure
– Uso sicuro di Internet e posta elettronica
– Uso sicuro dei sistemi di protezione dai virus
– Struttura di archiviazione dei documenti
La carta da sola non basta! I collaboratori vanno • sensibilizzati periodicamente sulla problematica della sicurezza.

Consigli e suggerimenti

Disciplinate l'installazione e l'uso di programmi e • hardware propri (giochi, screensaver, chiavette USB, modem, notebook privati, wireless LAN, computer palmari, ecc.).
Disciplinate l'uso di Internet: che cosa possono o • non possono scaricare i collaboratori (informazioni, programmi, ecc.)?
Vietate l'accesso alle chat room così come alle • pagine Internet con contenuti pornografici, razzistie violenti.
Stabilite le modalità di backup dei dati, soprattutto • per gli utenti di notebook (vedi punto 2).
Disciplinate la gestione delle password (vedi • punto 6).
Disciplinate la gestione degli aggiornamenti di sicu• rezza e dei programmi antivirus (vedi punti 3 e 5).
Disciplinate l'uso delle e-mail: nessun dato riservato, • nessun inoltro all'indirizzo di posta elettronica privato, nessun messaggio a catena, ecc.
Disciplinate la gestione delle informazioni e dei dati • riservati e stabilite una modalità di archiviazione protetta per i dati.
Disciplinate il comportamento da seguire in caso • di eventi importanti per la sicurezza, come le segnalazioni di virus o i furti e le perdite di notebook e password.
Preannunciate sanzioni in caso di violazione delle • linee guida per l'utente.

Proteggete l’ambiente della vostra infrastruttura IT!

Sapete chi entra ed esce dalla vostra azienda durante il giorno? Bastano poche precauzioni per impedire che persone non autorizzate accedano a informazioni aziendali importanti. Misure di sicurezza concrete e visibili sono oggi un criterio di qualità e generano fiducia nei clienti e nei fornitori. A cosa serve anche il migliore dei firewall se uno sconosciuto può introdursi nei vostri uffici?

Tutti gli accessi all’edificio o alla superficie coperta • dalla vostra impresa devono essere chiusi a chiave oppure sorvegliati. Se ciò non fosse possibile, occorre proteggere almeno la sezione degli uffici.

Non lasciate andare in giro per la vostra azienda • senza sorveglianza visitatori, clienti e conoscenti.

Tutte le terze persone devono essere accolte • all’ingresso, accompagnate per tutta la durata della loro permanenza e congedate all’uscita quando lasciano l’edificio.

Se non disponete di un servizio di accoglienza che • sorvegli l’area dell’ingresso occorre chiudere le porte e affiggere un cartello con scritto «Si prega di suonare».

Assicuratevi che tutti i possibili accessi (finestre, • porte, ecc.) dispongano di una sufficiente protezione antiscasso. Schede informative sull’argomento sono disponibili presso qualsiasi stazione di polizia.

Le chiavi e i badge devono essere amministrati • correttamente, tenendo aggiornate le rispettive liste. Le chiavi passe-partout vanno distribuite con forti limitazioni, e almeno una volta all’anno è necessario verificare la necessità delle rispettive autorizzazioni.

All’uscita dall’impresa i collaboratori riconsegnano • le loro chiavi, i badge e altre forme di autorizzazione all’accesso.

Consigli e suggerimenti

Collocate i server all’interno di locali climatizzati che • si possono chiudere a chiave. Se non è disponibile una sala adeguata, chiudete i server all’interno di un armadio per computer (rack).

Non conservate materiali infiammabili come carta, • ecc. all’interno o nelle immediate vicinanze della sala server.

Nella sala server collocate, in posizione ben visibile, • un estintore a CO2.

Non collocate le stampanti di rete nelle sale acces• sibili al pubblico, poiché persone non autorizzate potrebbero leggere i documenti.

Proteggete i cavi di rete che attraversano i locali • pubblici e chiudete sotto chiave modem, hub, router e switch.

Tenete in ordine i documenti e i supporti dati!

Quanto è importante l'ordine per la sicurezza? Più di quanto si potrebbe pensare. Se la postazione di lavoro è ordinata, vi sono meno probabilità che dati e documenti vadano persi rispetto a un piano di lavoro cosparso di carte, foglietti e cartelline.

Una chiara politica riguardo all'ordine riduce al mi• nimo il pericolo che documenti sensibili finiscano sotto gli occhi sbagliati o vengano letti per caso da persone non autorizzate.

L'ordine è anche una questione di immagine: in • base all'ordine esteriore clienti e fornitori tendono infatti a trarre delle conclusioni anche sull'atteggiamento interiore.

Ordinate i dati elettronici e i documenti cartacei • con un sistema di archiviazione uniforme, per es. per cliente o progetto. Il sistema deve avere una struttura logica ed essere di facile comprensione per i collaboratori.

Se si devono portare dei dati fuori sede, è oppor• tuno utilizzare supporti nuovi, mai utilizzati. Le informazioni cancellate in maniera tradizionale, infatti, possono essere ripristinate con relativa semplicità, e persone non autorizzate potrebbero leggerle. L'unico modo per cancellare i dati in modo affidabile consiste nell'uso di un programma«wipe». Trovate ulteriori informazioni al riguardo in Internet.

Se al computer lavorate con dati sensibili posizio• nate lo schermo in modo che colleghi e visitatori non possano leggere le informazioni visualizzate.

Consigli e suggerimenti

Cancellate i dati non più necessari presenti su sup• porti come CD, DVD, chiavette USB e dischi rigidi sovrascrivendo l'intera area di memorizzazione. Il comando Elimina non basta! La soluzione migliore consiste nel distruggere fisicamente i supporti prima di smaltirli.

Conservate sempre sotto chiave i documenti riser• vati, per esempio quelli contenenti dati personali.

Eliminate in modo sicuro i documenti cartacei non • più necessari e gli appunti contenenti dati sensibili (distruggidocumenti).

Durante le pause e le assenze dalla postazione di • lavoro bloccate il computer con una password e chiudete sotto chiave i documenti dal contenuto riservato.

Non lasciate i documenti stampati sulla stampante. • Questa regola vale in particolare per le aree accessibili al pubblico (accoglienza, ecc.).

10 ulteriori punti per una maggiore riservatezza e disponibilità!

Volete sapere se la vostra impresa mette in atto misure di sicurezza elevate e se ha bisogno di ulteriori provvedimenti di sicurezza? I punti seguenti vi aiuteranno a stimare la necessità di attuare ulteriori misure, che troverete descritte nelle prossime pagine.

Proteggete la vostra impresa con ulteriori misure per la **riservatezza** se

requisiti di legge, disposizioni o contratti esigono esplicitamente condizioni di riservatezza (per es. Legge sulla • protezione dei dati, Legge sul diritto d'autore);

l'eventuale abuso di dati riservati potrebbe comportare gravi perdite finanziarie o seri danni in termini di • immagine o fiducia, per es. in caso di pubblicazione di segreti aziendali o di offerte;

l'eventuale abuso di dati personali influenzerebbe notevolmente la posizione sociale o le condizioni eco• nomiche della persona in questione, per es. in caso di pubblicazione di dati riservati sulla clientela;

la vostra impresa necessita in generale di lavorare in condizioni di riservatezza. È il caso, per esempio, di • imprese di consulenza per il personale, associazioni, ospedali, amministratori fiduciari, studi medici e legali.

Nelle prossime pagine prestate particolare attenzione ai punti da 11 a 15.

Proteggete la vostra impresa con ulteriori misure per la **disponibilità** se

in caso di guasto ai sistemi IT la vostra impresa ne risentirebbe così tanto da generare un notevole danno • complessivo (per es. ritardi nella consegna per una gestione non puntuale degli ordini);

un eventuale guasto alle applicazioni IT provocherebbe seri danni in termini di immagine o fiducia (per es. • malfunzionamento del sistema di prenotazioni per una società di viaggi, rottura del server Web per i clienti);

il mancato funzionamento dell'applicazione o del sistema IT metterebbe immediatamente a rischio l'integrità • personale delle persone (per es. inaffidabilità del sistema di chiusura);

la vostra impresa necessita in generale di operare con buoni livelli di disponibilità. È il caso, per esempio, di • imprese di produzione e commercio, tipografie o negozi online.

Nelle prossime pagine prestate particolare attenzione ai punti da 16 a 20.

www.isss.ch

Rispettate le disposizioni!

Un'impresa deve rispettare diverse disposizioni in materia di riservatezza. Oltre alle disposizioni di legge, si può trattare anche di contratti o regolamenti. L'inosservanza di queste norme può avere conseguenze legali e provocare una perdita di immagine per l'impresa.

Occorre rispettare in particolare la Legge sulla• protezione dei dati (LPD), la Legge sul dirittod'autore (LDA) e il diritto delle obbligazioni (CO).

Se si elaborano in qualche modo dati relativi a • persone, come clienti o collaboratori, si applica la Legge sulla protezione dei dati. In base a questa legge i dati devono essere protetti da elaborazioninon autorizzate con adeguate misure tecniche e organizzative. Oltre a questo occorre garantire anche la correttezza contenutistica dei dati raccolti.

È necessario rispettare anche i contratti con • clientie partner, in quanto possono contenere accordi speciali in merito alla riservatezza.

Consigli e suggerimenti

Studiate le leggi e le ordinanze pertinenti, e adottate • le precauzioni necessarie per rispettarle.

Prestate attenzione affinché i dati vengano raccolti • in maniera ineccepibile dal punto di vista legale e siano memorizzati correttamente.

Permettete alle persone in questione di ottenere • informazioni sui dati memorizzati su di loro.

Ulteriori informazioni si trovano sul sito • dell'Incaricato federale della protezione dei dati e della trasparenza (http://www.edoeb.admin.ch/) e sul sito dell'Incaricato della protezione dei dati del Canton Zurigo (http://www.datenschutz.ch).

L'analisi del bisogno di protezione dell'Organo stra• tegia informatica della Confederazione (OSIC) è utile per valutare correttamente la sicurezza in ambito informatico (http://www.isb.admin.ch/themen/sicherheit/00151/00174/index.html).

Disciplinate la protezione dell’accesso ai dati!

Accessi non autorizzati possono portare ad abusi delle informazioni. Proteggete quindi l’accesso ai dati in modo da riservarlo soltanto alle persone autorizzate.

Se una persona non autorizzata accede alle • informazioni può visualizzare, copiare, modificare o cancellare i dati, con conseguenze gravi. Immaginate se un’offerta finisse nelle mani sbagliate, la vostra banca dati dei clienti venisse cancellata o i risultati delle vostre ricerche giungessero sulla scrivania della concorrenza.

Stabilite chi ha accesso a determinate applicazio• ni IT o informazioni. I diritti d’accesso andrebbero quindi distribuiti conformemente ai vari ruoli, per es. segreteria, vendite, contabilità, personale, amministratore di sistema.

Vanno concessi soltanto i diritti d’accesso neces• sari per consentire l’esecuzione di un compito («principio need-to-know»).

I diritti d’accesso vengono assegnati dall’ap• posita amministrazione del sistema IT o da un’amministrazione utenti sovraordinata.

Consigli e suggerimenti

Introducete un sistema di classificazione per le • vostreinformazioni.

I diritti d’accesso vengono stabiliti dalla persona di • volta in volta responsabile.

L’amministrazione dei diritti deve essere docu• mentata, stabilendo quale persona riveste quale funzionee quale persona ha accesso a quali applicazioni e dati. Verificate periodicamente tali diritti e adeguateli di conseguenza

Utilizzate un sistema di autenticazione sicuro: oltre • al nome utente e alla password potete utilizzare per esempio un terzo elemento di sicurezza, come una smart card.

Quando un collaboratore lascia l’impresa o cambia • ruolo al suo interno il rispettivo account utente e i diritti d’accesso vanno bloccati o adeguati immediatamente.

Particolare attenzione va prestata per i gestori • di sistema e gli amministratori, che solitamente dispongono di diritti molto ampi.

Cifrate i supporti dati mobili e le trasmissioni!

Se la trasmissione non è protetta (per es. e-mail) i dati riservati possono essere visionati da terze persone. I dispositivi mobili possono andare persi e i loro dati possono finire nelle mani sbagliate. Per garantire la riservatezza è necessario quindi cifrare tanto i dati sui dispositivi quanto le trasmissioni.

I messaggi di posta elettronica possono essere • letti da terze persone. Per questo motivo occorre cifrare le e-mail dal contenuto riservato.

Se memorizzate dei dati riservati – in particolare • su dispositivi mobili come notebook, smartphoneo agende digitali – bisogna applicare una soluzione di crittografia che consenta di decifrare l'informazione solo con la relativa password o chiave.

Consigli e suggerimenti

Stabilite delle regole per la cifratura, indicando • quali dati e quali dispositivi della vostra impresa devono essere crittografati. Istruite i vostri collaboratori su come utilizzare la crittografia. Stabilite delle regole anche per la decifratura, affinché in futuro sia comunque possibile accedere ai dati archiviati anche se i collaboratori che li hanno cifrati lasciano l'impresa.

Installate un software di crittografia su tutti i dispo• sitivi che contengono dati sensibili. La crittografia deve essere protetta da una password sicura (vedi punto 6).

Utilizzate un software di crittografia per le comuni• cazioni e-mail contenenti dati sensibili.

Una semplice soluzione consiste nel comprimere • i dati sensibili all'interno di una cartella zip e crittografarli. Prestate attenzione a non trasmettere la password sullo stesso canale di comunicazione (per es. file zip via e-mail, password per SMS).

Potete usare anche il prodotto Pretty Good Privacy • (PGP). Si tratta di un software molto diffuso che dispone di funzioni tecnologicamente avanzate per la crittografia, la firma digitale e l'eliminazione sicura di dati. Il programma PGP per usi commerciali si trova sul sito Web ufficiale http://www.pgp.com/de/index.html.

Per usare la versione standard e gratuita OpenPGP • visitate il sito http://www.gnupg.org/index.it.html.

Trattate con riservatezza anche i dati non elettronici!

Ciò che vale per i dati elettronici si applica ovviamente anche ai dati in formato cartaceo o alle comunicazioni a voce: mettete tutti in guardia, proteggete i dati riservati e non permettete le chiacchiere.

Ogni documento ha un proprietario e un archivio, • i documenti devono essere classificati, i diritti sui documenti devono essere assegnati e in caso di mancato utilizzo le informazioni vanno eliminate correttamente.

I documenti cartacei riservati vanno conservati in • un luogo sicuro. E sicuro significa «sotto chiave».

I documenti cartacei riservati devono essere elimi• nati con un distruggidocumenti.

Anche le comunicazioni a voce vanno trattate con • riservatezza, per es. quando si parla in pubblico. Avvertite i vostri collaboratori dei rischi in cui si incorre parlando di informazioni riservate in un luogo pubblico.

Sensibilizzate i vostri collaboratori sugli aspetti del • social engineering (manipolazione di persone allo scopo di ottenere informazioni protette) e dello spionaggio. I dati riservati non vanno mai trattati con leggerezza e superficialità.

Consigli e suggerimenti

Classificate anche i vostri documenti in formato • cartaceo.

Ovunque si elaborano dati riservati deve essere • disponibile anche un distruggidocumenti.

Create le possibilità per conservare i documenti • in modo sicuro, per es. con armadi per le pratiche chiudibili separatamente.

Conservate i documenti dal contenuto riservato in • un armadio chiudibile a chiave o in cassaforte. Questo vale tanto per i documenti in formato cartaceo quanto per i supporti dati.

Sensibilizzate i vostri collaboratori!

Solo se vengono sensibilizzati i collaboratori mettono in pratica le misure di sicurezza. Spiegate ai vostri collaboratori la necessità delle misure e della gestione corretta dei dati riservati. Eventualmente stipulate un accordo sulla riservatezza.

I collaboratori propri ed esterni trattano spesso • dati riservati. Queste persone devono sapere che devono attuare misure adeguate per garantire la riservatezza.

Inserite una clausola sulla riservatezza all'interno • del contratto di lavoro, anche in caso di collaboratori esterni e partner. L'accordo sulla riservatezza definisce il modo in cui vanno trattate le informazioni riservate. Sottolineate le conseguenze del mancato rispetto dell'accordo.

Illustrate alle persone interessate le basi legali • di questi provvedimenti (per es. la Legge sulla protezione dei dati).

Consigli e suggerimenti

Sensibilizzate i nuovi collaboratori riguardo all'im• portanza della sicurezza informatica già al momento dell'assunzione.

La sensibilizzazione è un processo continuo. Per • questo occorre organizzare periodicamente delle campagne sulla sicurezza, per es. sotto forma di corsi di formazione, sondaggi, promemoria, opuscoli, ecc.

Potete avvalervi delle opportunità offerte da terzi,• come l'associazione ISSS http://www.isss.ch.

Controllate i vostri sistemi!

È necessario garantire sempre un corretto funzionamento dei sistemi IT. Per questo occorre controllarli ed eseguire una manutenzione regolare se si vogliono ridurre gli inconvenienti tecnici e prevenire i danni alle strutture informatiche.

- Verificate periodicamente l'efficienza dei vostri sistemi IT: il sistema di backup funziona? I dati del backup sono effettivamente leggibili? Il gruppo di continuità (UPS) funziona? I file automatici del registro di sistema contengono messaggi d'errore?
- Prestate attenzione anche agli aspetti organizzativi: le linee guida legali e di altro genere vengono rispettate? Il piano d'emergenza è stato verificato?
- La manutenzione dei dispositivi e dei sistemi può essere eseguita da voi stessi, oppure potete affidarla a partner (per es. ai produttori). Nel caso di partner esterni assicuratevi che siano persone affidabili e assegnate soltanto diritti d'accesso e di ingresso limitati.
- Le operazioni di monitoraggio e manutenzione vanno eseguite a intervalli regolari.

Consigli e suggerimenti

- Redigete un elenco di manutenzione: chi deve eseguire il controllo e la manutenzione su cosa, e quando? Garantite il monitoraggio e la tracciabilità delle attività di manutenzione.
- Fino a un certo livello il monitoraggio dei sistemi può essere automatizzato, per es. impostando il software affinché invii automaticamente un messaggio d'errore all'amministratore quando viene superato un valore critico.
- Fate firmare ai tecnici esterni della manutenzione un accordo sulla riservatezza.
- L'accesso ai dati e alle informazioni da parte di esterni va il più possibile evitato.
- Informate le persone interessate delle attività di manutenzione previste.

Garantite un approvvigionamento elettrico senza interruzioni!

Se dovete garantire una disponibilità elevata per i vostri dati e sistemi, non potete permettervi nessun tipo di malfunzionamento. Un gruppo di continuità (UPS) proteggei vostri sistemi dalle interruzioni nell'alimentazione elettrica e dalle sovratensioni (provocate per esempio da un fulmine) prevenendo le perdite di dati.

Il gruppo di continuità (UPS) va installato tra la • presa di corrente normale e i dispositivi da proteggere.

In caso di interruzione nella fornitura di corrente • elettrica, la batteria del gruppo di continuità alimenta i vari componenti per il tempo necessario a spegnerli correttamente.

Inoltre un gruppo di continuità può fungere da • filtro e proteggere i vostri sistemi dalle sovratensioni.

Oltre al server bisogna collegare al gruppo di con• tinuità anche altre periferiche importanti, tra cui i computer principali della rete, il router, i sistemi di backup, ecc.

Consigli e suggerimenti

Redigete un elenco dei componenti che devono • esserecollegati al gruppo di continuità. In base alla configurazione richiesta si determinerà quindi la potenza necessaria per lo stesso.

Verificate periodicamente la potenza delle batterie • del gruppo di continuità e sostituite immediatamente le batterie quasi scariche (vedi punto 16).

Garantite la ridondanza degli elementi importanti!

Il mancato funzionamento di un elemento critico della vostra rete, come per esempio un server, può comportare ingenti danni economici e interrompere l'attività produttiva. Molte imprese non sono consapevoli di quanto dipendono dai sistemi critici. Per poter riprendere le attività il prima possibile in seguito a un guasto si consiglia di puntare sulla ridondanza dei sistemi IT critici (per es. disco rigido, alimentatori, componenti di rete o interi server).

Ridondanza significa poter disporre di almeno un • dispositivo o sistema sostitutivo identico che possa rimpiazzare l'elemento danneggiato in caso di guasto.

Per rimediare alla rottura di un disco rigido si può • utilizzare una cosiddetta immagine dell'hard disk. In caso di malfunzionamento, infatti, gli altri dischi rigidi possono sostituirlo automaticamente nello svolgimento delle sue funzioni senza interrompere l'attività produttiva.

Stipulate con i vostri fornitori dei contratti di servi• zio per gli interventi hardware e software (tempi di risposta, scadenze di consegna, ecc.).

Eventualmente predisponete con il vostro fornitore • dei piani d'emergenza per i guasti (vedi punto 19).

Consigli e suggerimenti

Utilizzate soltanto componenti di produttori rino• mati. Solitamente sono di buona qualità e hanno superato test approfonditi.

Preoccupatevi di rendere ridondanti non soltanto i • sistemi IT, ma anche il collegamento a Internet.

L'importante è che i dispositivi sostitutivi siano iden• tici e preconfigurati, così da poter essere utilizzati immediatamente all'occorrenza.

Predisponete un piano d'emergenza!

Generalmente i casi di emergenza gravi si verificano all'improvviso, e soprattutto nei casi di forza maggiore si rimane del tutto inermi. Se si reagisce correttamente a una situazione di emergenza è possibile contenere i danni, e per questo motivo occorre stabilire in anticipo come comportarsi nelle emergenze e quali misure attuare.

Pensate a quali situazioni di emergenza potreb• bero verificarsi nella vostra impresa e a come bisognerebbe reagire. Analizzate gli scenari problematici seguenti: guasto IT, assenza di personale, problemi alle postazioni di lavoro o all'edificio e mancata disponibilità di partner e servizi esterni.

In caso di emergenza l'allarme e le reazioni devono • essere rapidi. Ogni persona deve sapere di preciso a chi va notificato l'allarme e a chi spetta la competenza. Redigete a tal fine un piano per gli allarmi e un regolamento delle responsabilità.

Redigete un piano che comprenda interventi im• mediati per l'avvio delle attività in emergenza, regole per lo svolgimento delle stesse in questi casi e provvedimenti per ripristinare rapidamente il normale funzionamento dell'azienda.

Illustrate ai collaboratori il comportamento da • assumere nei casi di emergenza e le misure immediate che devono essere attuate.

Nelle situazioni di stress le persone tendono a • comportarsi istintivamente. Per questo motivo i comportamenti da seguire in caso di emergenza vanno acquisiti tramite esercitazioni.

Eventualmente potrebbe essere utile stipulare • delle assicurazioni IT per i grandi rischi, per es. un'assicurazione impianti o un'assicurazione complementare per i costi dei supporti dati e del ripristino.

Consigli e suggerimenti

Documentate accuratamente tutti i componenti IT. • Conservate questa documentazione al di fuori della sede.

Organizzate le possibilità di ripiego per i sistemi • IT con i maggiori requisiti di disponibilità, così da garantire un rapido proseguimento delle attività.

Verificate i tempi di risposta del supporto in base ai • vostri requisiti di disponibilità. Un danno subito dal server, per esempio, può davvero essere risolto nei tempi necessari?

Elaborate con il fornitore e i produttori dei piani • d'emergenza per i guasti (vedi punto 18).

Distribuite il know-how!

Proprio nelle PMI più piccole le competenze fondamentali in materia di sistemi IT sono spesso possedute da una sola persona. Se questa è assente o lascia l'impresa, sorgono dei problemi.

Le conoscenze chiave riguardano la configurazione, il funzionamento e la manutenzione dei sistemi IT dell'impresa.

Malattia, infortunio, decesso o abbandono dell'impresa possono portare alla perdita del know-how chiave.

Cercate di distribuire e documentare le conoscenze fondamentali delle persone.

Consigli e suggerimenti

Per evitare di perdere l'accesso al know-how in caso di assenza, è opportuno documentare i sistemi e i processi principali. In questo modo si consente anche ai successori e ai nuovi collaboratori di orientarsi più facilmente.

La documentazione dovrebbe comprendere per esempio un elenco di utenti, gruppi e diritti (vedi punto 12), l'architettura di rete, le configurazioni dei sistemi, la descrizione delle installazioni, progetti, flussi di lavoro e una descrizione degli incarichi per le funzioni importanti in termini di sicurezza. Aggiornate regolarmente questa documentazione.

Utilizzate regole omogenee per denominare i documenti e contrassegnateli con numero di versione, data, motivi per la revisione e nome dell'autore.

Mettete su carta uno schema della rete con i rispettivi server e componenti.

Conservate una copia delle password importanti all'interno di una cassaforte.

Salvate i dati importanti per l'attività aziendale elaborati dagli ex collaboratori.

Glossario

ADSL Connessione rapida a Internet. Con l'ADSL un computer è sempre collegato a Internet e può essere attaccato in qualsiasi momento. Come protezione minima è opportuno impiegare un *firewall*.

Antivirus Programma che protegge il computer identificando ed eliminando i *virus* informatici e altri programmi dannosi per il computer, come *worm* e *cavalli di Troia*. Vedi anche *malware*.

Attachment (allegato) File allegato a un messaggio di posta elettronica. Molti programmi dannosi (*malware, crimeware*) si diffondono in questo modo e vengono attivati aprendo il messaggio o l'allegato. È quindi opportuno aprire un allegato solo se si usa un *antivirus* e si conosce il mittente del messaggio.

Audit Indagine tramite la quale viene verificato se i sistemi e i processi impiegati in un'impresa sono conformi ai requisiti e alle linee guida.

Backup Procedimento per cui salvando i dati su supporti di memorizzazione esterni se ne previene l'eventuale perdita.

Bluetooth Trasmissione radio a corto raggio che può essere utilizzata da computer portatili e telefonini per lo scambio di dati.

Browser Programma utilizzato per consultare le informazioniin Internet (per es. Internet Explorer, Opera o Firefox).

Cavallo di Troia Pericoloso programma *malware* che viene salvato ed eseguito sul computer generalmente senza che l'utente se ne renda conto o dia il suo consenso. Nella maggior parte dei casi instaura una comunicazione con un malintenzionato (*cracker*) per conferirgli il totale controllo sul computer. Come protezione minima è opportuno impiegare un *antivirus*.

Chiavetta USB Detta anche «pen drive» o «memory stick». Supporto di memorizzazione che si collega alla porta USB del computer. Date le dimensioni contenute e l'ampia capacità di memorizzazione questi supporti vengono utilizzati anche dai ladri di dati.

Client Computer connesso a una rete e collegato con altri computer.

Cracker *Hacker* che sfrutta le sue competenze e la sua esperienza per arrecare danno agli altri.

Crimeware Termine collettivo per tutti i programmi utilizzati da *cracker* e altri criminali informatici per danneggiare altri utenti informatici. Solitamente l'obiettivo del crimeware è quello di impossessarsi di denaro o informazioni preziose (per es. numeri di carte di credito). Una forma meno aggressiva viene denominata *spyware*.

Download (scaricamento) Processo attraverso il quale si salvano sul proprio computer dati e programmi che si trovanosu un computer distante (per es. in Internet).

Firewall («parete tagliafuoco») Dispositivo o programma informatico che protegge computer o reti dagli accessi non autorizzati provenienti dall'esterno (per es. a opera di *cracker*).

Firma digitale Firma digitale di natura vincolante.

Gruppo di continuità (UPS, dall'inglese «Uninterruptible Power Supply») Dispositivo collocato tra la presa di corrente e l'utilizzatore che in caso di interruzione nella fornitura di elettricità funge da batteria di supporto, oltre a proteggere dalle sovratensioni grazie alla sua funzione di filtro.

Hacker Specialista che dispone di un'enorme conoscenza dei computer e delle reti ed è in grado di riconoscere e sfruttare gli errori presenti. A differenza dei *cracker* gli hacker non operano per fini illegali.

Hub Dispositivo cui si possono collegare diversi computer per formare una piccola rete.

Indirizzo IP Indirizzo numerico che identifica in modo univoco i dispositivi di una rete (per es. Internet).

Instant Messenger Programma con cui si possono scambiare brevi messaggi di testo in tempo reale.

ISDN Rete di telecomunicazioni digitale per la trasmissione di voce e dati a velocità e in condizioni di sicurezza superiori rispetto alla tecnologia analogica.

Junk mail (posta indesiderata) Posta elettronica non desiderata, solitamente pubblicità; viene indicata anche con il termine inglese *spam*.

Login Accesso a un servizio, eseguito solitamente con l'inserimento di un *nome utente* e di una password.

Malware Detto anche «Malicious Code». Termine collettivo per i programmi nocivi e dannosi, come *virus*, *worm* o *cavalli di Troia*.

Modem Dispositivo che converte i segnali elettrici in suoni e viceversa. Viene utilizzato per instaurare una connessione a reti digitali (per es. Internet) attraverso cavi telefonici analogici. Denominato anche *modem ADSL* o *modem via cavo*.

Modem via cavo Dispositivo per l'accesso a Internet attraverso la rete della televisione via cavo.

Nome utente (username) Viene utilizzato solitamente in combinazione con una password per accedere a un servizio (per es. Internet) o a un programma.

Patch («toppa») Aggiornamento di programmi in cui sono stati trovati degli errori. Vedi anche *update*.

PGP (Pretty Good Privacy, italiano: «sfera privata piuttosto buona») Programma per la crittografia dei dati.

Pharming Attacco di *phishing* avanzato nel quale il computer della vittima viene manipolato in modo tale da rendere riconoscibile l'attacco stesso soltanto agli occhi di professionisti in materia di sicurezza o di rete. Alla luce di questa tipologia di attacchi sono vivamente consigliati l'uso di un *antivirus* e di un *firewall* e l'installazione quotidiana delle *patch* disponibili.

Phishing Metodo di attacco che mira a ingannare una vittima affinché riveli i dati di *login* per servizi finanziari (per es. e-banking); avviene via e-mail oppure tramite la visitaa una pagina Internet contraffatta dall'aspetto identico all'originale.

Provider Fornitore di accesso a una rete (per es. Internet). Noti provider sono Bluewin, Sunrise o Cablecom.

Remote Access Accesso remoto a una rete o un computer, solitamente tramite Internet. Tali accessi andrebbero resi possibili solo con l'ausilio di tecnologie di sicurezza come *firewall* e *VPN*.

RM Acronimo di *Risk Management*. Gestione sistematica dei rischi di un'impresa (analisi, misure, controllo).

Router Dispositivo che collega le reti tra di loro. Detto anche router *ADSL*.

SCI Acronimo di *Sistema di controllo* interno ai sensi dell'art. 728a (CO); insieme di tutte le misure di controllo attuate in un'impresa per raggiungere gli obiettivi aziendali.

Server Computer che all'interno di una rete mette a disposizione degli altri computer (*client*) alcuni servizi (per es. server di posta elettronica).

Sistema operativo Software di sistema, indicato anche con la sigla inglese «OS» (Operating System). Si tratta di una raccolta

Smart Card Scheda di plastica contenente un chip in grado di memorizzare dati cui si può accedere tramite l'inserimento di un codice (PIN).

Spam Messaggi di posta elettronica di massa inviati come catene di S. Antonio o pubblicità per prodotti o servizi particolari o di dubbia natura. Con un filtro antispam è possibile proteggersi da tali messaggi e dividere una buona parte della posta indesiderata dai messaggi in arrivo.

Spyware Tipo di *malware* utilizzato per spiare il comportamento di utenti di computer. Vengono osservati in particolare il comportamento dell'utente in Internet e i tasti premuti sulla tastiera (furto di password!). Come protezione si consiglia l'uso regolare di uno spyware scanner.

Switch Dispositivo che collega tra di loro computer o reti. Viene utilizzato nelle reti locali (LAN).

Update Routine di aggiornamento che ripara i programmi contenenti errori (per es. i *sistemi operativi*). Vedi anche patch.

URL Indirizzo di una pagina in Internet, per es. www.isss.ch.

disco floppy, CD-ROM, chiavetta USB, e-mail, ecc.) e richiede un'azione dell'utente per essere attivato. Come forma di protezione è opportuno impiegare un *antivirus* regolarmente aggiornato e attivato.

VPN (Virtual Private Network) Tecnologia che tramite l'impiego di soluzioni di crittografia e controlli d'accesso (*login*) rende possibile l'uso sicuro di reti pubbliche (per es. Internet) per fini privati.

Worm Programma dannoso (*malware*) che senza l'intervento di terzi sfrutta i punti deboli o gli errori dei programmi per diffondersi attraverso le reti e bloccare temporaneamente tanto le reti quanto i computer connessi. Spesso i worm contengono anche comandi che distruggono i dati. Come protezione minima è opportuno impiegare un *antivirus*.

Zombie Computer assoggettato al controllo di una terza persona (per es. un *cracker*) per mezzo di un *cavallo di Troia*; generalmente viene sfruttato per sferrare attacchi ad altri computer collegati in Internet.

www.isss.ch

ISSS Information Security Society Switzerland
Bollwerk 21
CH-3001 Bern
T +41 31 311 5300
sekretariat@isss.ch
www.isss.ch