Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale delle finanze DFF
Segreteria generale

Centro nazionale per la cibersicurezza NCSC
www.ncsc.admin.ch

NCSC

Promemoria sulla sicurezza delle informazioni per le PMI

Sommario

1 Introduzione

Il presente promemoria è rivolto alle PMI svizzere e ha lo scopo di aiutarle a migliorare la sicurezza dell'informazione all'interno della loro impresa[1].

Il promemoria è suddiviso in:

- **misure organizzative**, volte a migliorare o a garantire la sicurezza dell'informazione;
- **misure tecniche**, volte a migliorare o a garantire la sicurezza dell'infrastruttura informatica.

Le misure tecniche contribuiscono in modo essenziale a garantire la sicurezza dell'informazione, ma devono essere completate da provvedimenti di carattere organizzativo. In particolare quando si tratta di misure molto onerose in termini di costi e/o di personale, ogni impresa deve soppesare i costi del provvedimento e i rischi in cui incorre se quest'ultimo non viene adottato. Le misure non attutate comportano i cosiddetti «rischi residui», che la direzione deve decidere se accettare, oppure predisporre le risorse necessarie per minimizzarli. Sebbene i rischi di carattere tecnico dei sistemi informatici rappresentino una parte importante della sicurezza dell'informazione, un'impresa non dovrebbe focalizzare la sua attenzione unicamente su questa parte dei rischi o addirittura definire la divisione IT come l'unica soggetta a rischi. La responsabilità della gestione dei rischi, la classificazione delle informazioni così come l'impiego graduale delle misure di sicurezza a disposizione rientrano tra i compiti principali della direzione.

1.1 Misure organizzative

Le misure di carattere organizzativo garantiscono che le responsabilità riguardanti la sicurezza delle informazioni all'interno dell'impresa siano definite.

Informazioni della direzione sui rischi
Valutate la dipendenza dei vostri processi operativi dal vostro sistema informatico. Ponetevi ad esempio le domande seguenti: quali conseguenze potrebbe avere il guasto di un sistema o l'inaccessibilità di una banca dati? Quali sono le possibili conseguenze finanziarie? Quali misure possono essere adottate per evitare che accada? ecc.

I rischi come parte integrante della governance e della gestione della continuità operativa
L'attività operativa deve poter essere garantita anche se l'infrastruttura informatica o parte di essa è temporaneamente fuori uso, non necessariamente a seguito di un ciberattacco. Anche le interruzioni di corrente, eventi naturali o altri scenari possono causare guasti completi o parziali dell'infrastruttura IT. Definite per tempo possibili alternative e/o livelli di funzionamento ridotto dei sistemi.

Le responsabilità sono definite
I collaboratori devono sapere a chi rivolgersi in caso di domande sulla sicurezza informatica (ad es. quando ricevono e-mail sospette) o a chi comunicare un incidente legato alla sicurezza informatica. Elaborate tempestivamente un piano di gestione degli incidenti informatici («incident response plan»). Verificate regolarmente l'efficacia del piano, ad esempio con esercizi, e adeguatelo di conseguenza.

[1] V. anche «Informatica, informatica di sicurezza e infrastruttura: consigli» sul portale PMI della Confederazione: https://www.kmu.admin.ch/kmu/it/home/consigli-pratici/gestire-una-pmi/infrastruttura-e-it.html

Le competenze delle imprese e del fornitore di servizi IT
Molte piccole imprese affidano la parte informatica a un fornitore di servizi specializzato. Le competenze devono essere regolamentate in modo chiaro. Nel contratto definite anche le conseguenze in caso di violazione delle prescrizioni di sicurezza o di negligenza in questo ambito. Il contratto deve essere formulato in modo chiaro e univoco. A titolo di esempio, la mancata salvaguardia di dati a causa di un malinteso potrebbe avere conseguenze devastanti.[2]

Sensibilizzare i collaboratori
Sensibilizzare tutti i collaboratori all'uso dell'infrastruttura informatica è fondamentale. Istruite regolarmente il personale sulle regole da rispettare di fronte a potenziali rischi. Sul nostro sito Internet trovate le relative norme di comportamento.

Conoscenza della situazione attuale
Tenetevi aggiornati sulle nuove minacce in materia di sicurezza dell'informazione e sulle misure appropriate per affrontarle[3].

Trattamento dei dati sensibili
Stabilite regole vincolanti per la classificazione dei dati e applicatele in modo coerente. Disciplinate soprattutto il modo in cui i dati classificati elettronicamente devono essere salvati e/o trasmessi[4]. Definite direttive per la trasmissione delle informazioni aziendali. Di principio nessuna informazione confidenziale dovrebbe essere trasmessa tramite canali anonimi (ad es. telefono o e-mail).

Informazioni aziendali online
Spesso i criminali cercano informazioni sulle potenziali vittime. Riflettete quindi attentamente prima di pubblicare informazioni sul vostro sito web o sui social media. Riducete al minimo la quantità di informazioni relative all'impresa disponibili su Internet e valutate i rischi e i benefici. Emanate direttive in cui spiegate ai collaboratori come trattare le informazioni aziendali, ad esempio quando utilizzano i social media privatamente.

La sicurezza dall'acquisto allo smaltimento dell'infrastruttura IT
Le considerazioni relative alla sicurezza devono sempre essere integrate nel processo di acquisto. Occorre tenere conto dei requisiti per l'attivazione, ma anche dell'intero ciclo di vita di un sistema, incluse la manutenzione e la disattivazione. Prima dell'acquisto informatevi, ad esempio, sul modo in cui sono messi a disposizione gli aggiornamenti di sicurezza. Vengono installati automaticamente? Come viene comunicata la disponibilità di nuovi aggiornamenti? Definite la procedura per la disattivazione di parti dell'infrastruttura IT (ad es. come eliminare in modo sicuro le informazioni confidenziali dai sistemi).

Policy in materia di password
Definite regole vincolanti in materia di password e applicatele in modo coerente: la password deve essere lunga almeno 12 caratteri e comprendere lettere maiuscole e minuscole, numeri e caratteri speciali. Se possibile optate per l'autenticazione a due fattori. Evitate in ogni caso di utilizzare la stessa password più volte. Create una nuova password per ogni applicazione avvalendovi di un «password manager». Sul mercato trovate diversi sistemi – gratuiti o con

[2] Per ulteriori informazioni v. «Collaborazione con i fornitori di servizi IT»: https://www.ncsc.admin.ch/ncsc/it/home/infos-fuer/infos-unternehmen/aktuelle-themen/zusammenarbeit-it-provider.html

[3] Ogni sei mesi l'NCSC pubblica un rapporto sui principali ciberincidenti osservati in Svizzera e sul piano internazionale. Inoltre, sul sito dell'NCSC viene aggiornata regolarmente la classifica delle quattro minacce principali.

[4] Sul portale dell'incaricato federale della protezione dei dati e della trasparenza (IFPDT) trovate raccomandazioni e ordinanze in materia di protezione dei dati: https://www.edoeb.admin.ch/edoeb/it/home/protezione-dei-dati/visione-generale/protezione-dei-dati.html

licenza – per gestire le password su svariati sistemi operativi e dispositivi. Le password e i dati di accesso non devono mai essere comunicati a terzi.

Autorizzazioni di accesso
Pochissimi collaboratori hanno bisogno di diritti di amministratore estesi. Fornite ai collaboratori solo i diritti strettamente necessari allo svolgimento del loro lavoro (ad es. i collaboratori del marketing non hanno necessariamente bisogno di accedere alle informazioni della divisione del personale). In particolare, dovete bloccare i diritti per l'installazione di qualsiasi software.

e-banking
Per gli ordini di pagamento eseguiti in modo digitale (software per pagamenti offline, e-banking) servitevi di un computer dedicato, da non utilizzare per navigare in Internet o leggere e-mail. Regolamentate lo svolgimento del traffico dei pagamenti e attenetevi in modo coerente alle prescrizioni (principio del doppio controllo, firma collettiva, ecc.). Ciò vale soprattutto se più collaboratori sono autorizzati a eseguire pagamenti. È possibile disattivare o limitare le funzioni di e-banking non necessarie. Parlate con la vostra banca delle possibili misure di sicurezza, ad esempio riguardo all'eventuale blocco di alcuni Paesi.

1.2 Misure tecniche

Le misure di carattere tecnico non possono garantire una totale sicurezza. Spesso l'anello debole della catena non sono queste misure, bensì le persone. Se i collaboratori non vengono formati sul corretto approccio con i sistemi informatici in termini di sicurezza, l'efficacia delle misure tecniche descritte di seguito può risentirne pesantemente.

Salvaguardia regolare dei dati
Definite un processo per la regolare salvaguardia dei dati («backup») e applicatelo in modo coerente. Potete anche affidare la salvaguardia dei dati e altre misure tecniche a una ditta specializzata.

Verificate regolarmente che la savaguardia dei dati avvenga correttamente. Attivate periodicamente i backup in modo da familiarizzarvi con la procedura ed essere pronti in caso di necessità.

La copia di sicurezza deve essere salvata offline, ossia su un supporto esterno (ad es. un disco rigido esterno). Dopo aver eseguito il backup assicuratevi di scollegare fisicamente dal computer il supporto sul quale è stata salvaguardata la copia di sicurezza. In questo modo si evita che, in caso di attacco ransomware, i dati sul supporto di backup vengano criptati e resi inutilizzabili. Conservate anche i backup precedenti per un determinato periodo di tempo.

Protezione antivirus
Assicuratevi che su ogni computer sia installato un programma antivirus. È inoltre importante tenere il programma aggiornato ed eseguire regolarmente una scansione completa del sistema (ad es. a cadenza settimanale o mensile).

Firewall
Installate un firewall su ogni computer e proteggete la vostra rete aziendale contro i rischi provenienti da Internet con un firewall supplementare. Configurate il firewall in modo da definire il traffico dati in entrata e in uscita. Eseguite protocolli compatibili con i server proxy, quali ad esempio HTTP/HTTPS ecc. Analizzate regolarmente i log del proxy.

Aggiornamenti di sicurezza

Un software obsoleto è una delle porte di accesso preferite dai pirati informatici per gli attacchi malware. Assicuratevi che le misure di sicurezza si aggiornino automaticamente su tutti i computer e server della rete aziendale. Gli aggiornamenti di sicurezza di ogni software devono essere eseguiti non appena sono disponibili. Lo stesso vale per l'hardware, come stampanti, router ecc.

Sistemi di gestione dei contenuti (CMS)

I sistemi di gestione dei contenuti («content management systems», CMS) per la creazione e l'aggiornamento dei siti web devono essere sempre aggiornati. La maggior parte dei CMS ha una funzione di aggiornamento facilmente attivabile. Utilizzate un firewall per le applicazioni web («Web Application Firewall», WAF) per proteggere il vostro sito dagli attacchi. Sul sito dell'NCSC trovate un elenco di misure per proteggere i vostri CMS[5]. Se la vostra impresa dipende in misura importante dai siti web (ad es. un negozio online), pensate a come contrastare un eventuale attacco DDoS[6]. I grandi fornitori di servizi Internet in Svizzera offrono soluzioni per proteggersi contro gli attacchi DDoS che potete acquistare e pagare soltanto se ne avrete effettivamente bisogno.

File di log

I cosiddetti «file di log» («log file») sono cruciali nella risoluzione di incidenti informatici. Assicuratevi che i sistemi critici quali ad esempio il software di contabilità, il domain controller, il firewall o il server di posta elettronica supportino i file di log. Verificate regolarmente la presenza di anomalie nei file di log disponibili. Conservate i file di log per almeno sei mesi e includeteli nel vostro processo di backup. L'analisi dei file di log richiede conoscenze approfondite, è quindi opportuno affidarla a un fornitore di servizi informatici.

Segmentazione della rete[7]

Suddividete la rete aziendale in settori distinti (ad es. reti separate per la produzione, per il personale, per la contabilità). Non c'è alcun motivo per cui i collaboratori del servizio del personale debbano accedere al vostro ambiente di produzione. In questo modo evitate ad esempio che i computer di controllo di ambienti di produzione che non possono più essere aggiornati fungano da porta d'accesso per attacchi.

Almeno la contabilità e la divisione del personale dovrebbero avere una rete separata inaccessibile per gli altri computer collegati alla rete aziendale. Tenete presente che i malware possono diffondersi anche tramite la condivisione della rete. Chiedete consiglio al vostro fornitore di servizi per le fasi di pianificazione e attuazione.

Filtrare potenziali e-mail dannose

Le e-mail con allegati potenzialmente dannosi dovrebbero essere bloccate già dal gateway o intercettate dal filtro spam. Sul sito web dell'NCSC è disponibile un elenco di possibili estensioni dannose[8]. Dovrebbero essere bloccati anche allegati inviati come file di archivio (ad es. file .zip, .rar o .iso), inclusi quelli protetti (ad es. file .zip protetti da password).

---

5 Misure a protezione dei sistemi di gestione dei contenuti: https://www.ncsc.admin.ch/ncsc/it/home/infos-fuer/infos-unternehmen/aktuelle-themen/massnahmen-schutz-cms.html

6 Misure contro gli attacchi DDoS: https://www.ncsc.admin.ch/ncsc/it/home/infos-fuer/infos-unternehmen/aktuelle-themen/massnahmen-schutz-cms.html

7 V. ad es. il documento «Geeignete logische Segmentierung» dell'Ufficio federale tedesco per la sicurezza informatica: https://www.bsi.bund.de/DE/The- men/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05062.html (in tedesco)

8 Regole di comportamento dell'NCSC relative alle e-mail: https://www.ncsc.admin.ch/ncsc/it/home/infos-fuer/infos-unternehmen/aktuelle-themen/verhalten-bei-e-mail.html

Macro
Le macro servono essenzialmente per automatizzare documenti Office, ma vengono utilizzate anche per diffondere malware.
Si consiglia di bloccare tutti gli allegati che contengono macro (ad es. file Word, Excel o PowerPoint con macro). Sensibilizzate i collaboratori a non ignorare gli avvisi nei programmi Office.

Accessi remoti
L'accesso alla rete aziendale dall'esterno (ad es. viaggi d'affari, telelavoro ecc.) dovrebbe essere possibile solo tramite una rete privata virtuale (VPN) protetta da un'autenticazione a due fattori. Lo stesso vale per l'accesso di fornitori di servizi IT e amministratori esterni.

Servizi cloud
Grazie ai servizi cloud evitate di dover gestire internamente costose infrastrutture IT. Tuttavia, il loro utilizzo richiede prudenza. I dati sensibili dovrebbero sempre essere registrati solo localmente (mai su cloud!). Inoltre, prima di stipulare un contratto, informatevi presso il fornitore di servizi in merito alle principali misure di sicurezza (accesso ai dati, sicurezza dei dati ecc.).

Crittografia
Criptate i dati importanti, in particolare quando utilizzate servizi cloud e dispositivi mobili.