Manuale di audit CyberSeal

Version 1.5, 4 luglio 2023

Sommario

1 Obiettivo del documento

Questo manuale descrive in dettaglio l'applicazione della lista di controllo CyberSeal. Inoltre, vengono descritti il processo di audit, i costi, le condizioni quadro e ulteriori dettagli sull'assegnazione del marchio di conformità. Il manuale viene rivisto annualmente.

2 Il marchio di qualità Cyberseal

Una volta superato l'audit, l'Alleanza Sicurezza Digitale Svizzera ASDS conferisce al fornitore di servizi IT il marchio di qualità CyberSeal. Questo marchio di qualità conferma che il fornitore di servizi IT ha superato l'audit senza alcuna divergenza di rilievo.

Il marchio di qualità è valido per 3 anni a condizione che gli audit di manutenzione siano stati superati nei due e tre anni successivi.

Il marchio di qualità CyberSeal si basa sul fatto che la stragrande maggioranza delle PMI lavora a stretto contatto con un fornitore primario di servizi IT, in quanto una PMI non è generalmente in grado di garantire gli aspetti di configurazione e funzionamento sicuri delle tecnologie informatiche (IT) che sono oggi comuni e necessari. Pertanto, la sicurezza raggiunta da una PMI dipende in larga misura dal principale fornitore di servizi IT. Il marchio di qualità definisce gli aspetti di sicurezza che il fornitore di servizi IT deve implementare per sé e per i propri clienti. La PMI può fare affidamento sul fatto che un fornitore di servizi IT dotato del marchio di qualità CyberSeal tiene sufficientemente conto di aspetti importanti della cibersicurezza.

Durante l'audit CyberSeal, si risponde al questionario della lista di controllo CyberSeal. Le domande sono classificate in base alla rilevanza. La categorizzazione è stata scelta in modo che il marchio di qualità sia raggiungibile anche dai fornitori di servizi IT più piccoli.

In primo luogo, vengono presi in considerazione gli aspetti di sicurezza che sono centrali per le PMI e che sono spesso sfruttati da potenziali aggressori nell'ambiente delle PMI. Per lo sviluppo dello standard, sono molto importanti i rapporti delle compagnie di assicurazione e delle organizzazioni governative come l'NCSC (Centro Nazionale per la Cibersicurezza) sui danni effettivi verificatisi nell'ultimo anno. L'obiettivo è quello di affrontare le vulnerabilità più note e frequentemente sfruttate nelle PMI.

Il marchio di qualità CyberSeal ha un'elevata richiesta di attualità. Gli ultimi sviluppi in materia di aggressori e tipi di danni vengono incorporati ogni anno nello standard adattato.

Il marchio di qualità CyberSeal si differenzia per diversi aspetti dalle comuni etichette di sicurezza informatica, dagli altri marchi e dalle certificazioni (come la ISO/IEC 27001):

- Il marchio di qualità tiene conto del livello di integrazione delle tecnologie informatiche nelle PMI svizzere. Le PMI e i loro fornitori di servizi informatici sono particolarmente presi di mira.
- Il marchio di qualità garantisce che il fornitore di servizi IT adotta le misure di sicurezza più importanti per le comuni PMI. L'accento è posto sulla cibersicurezza.
- Il marchio di qualità è molto più facile da ottenere rispetto alla certificazione ISO/IEC 27001.
- Il marchio di qualità consente alle PMI di trovare un buon fornitore di servizi IT.
- Il marchio di qualità riflette l'attuale situazione di minaccia.

3 Nozioni di base

3.1 Condizioni

Fornitore di servizi IT: il fornitore di servizi IT è un'azienda che fornisce servizi IT a varie PMI. Il fornitore di servizi IT è quindi anche il punto centrale di fiducia per quanto riguarda la sicurezza informatica delle PMI. In Svizzera ci sono circa 5.000 aziende considerate fornitori di servizi IT.

PMI: una PMI è un'azienda di piccole o medie dimensioni. Per il marchio di qualità, si presume che una PMI sia piuttosto piccola e si affidi alle raccomandazioni di un fornitore di servizi IT in materia di sicurezza informatica.

Fornitori di servizi terzi: Altri fornitori di servizi incaricati dal fornitore di servizi IT o dalla PMI di fornire servizi. Il fornitore di servizi IT è responsabile dell'integrazione sicura di questo fornitore terzo. I fornitori terzi possono essere molto diversi tra loro: Fornitori di applicazioni (ad esempio Abacus), Dropbox, Office 365 e altri fornitori di cloud.

Auditor: un auditor nominato dall'organizzazione promotrice Alleanza Sicurezza Digitale Svizzera ASDS che può assegnare il marchio di qualità. L'ASDS può anche delegare la nomina dei revisori ad altre società di revisione (ad esempio SGS, BDO, ecc.).

Account privilegiato: Un account che dispone di autorizzazioni di sistema, di configurazione e/o di scrittura elevate.

Autenticazione a più fattori: per l'autenticazione vengono solitamente utilizzati due fattori diversi. In questo documento, sono inclusi sia i metodi comuni che utilizzano un token (SMS, Authenticator, ecc.) sia altri metodi, come gli intervalli di indirizzi IP limitati e i dispositivi protetti da certificati.

Autenticazioni multiple richieste (ad esempio, il login al sistema seguito da un login all'applicazione non sono considerate autenticazioni a più fattori).

Password forti: l'NCSC descrive sul sito web Protect your accounts / passwords (admin.ch) i requisiti delle password per essere considerate un'autenticazione abbastanza sicura**.**

Documentazione: la documentazione è qualsiasi forma di informazione reperibile, rintracciabile, rivista periodicamente e soggetta a una procedura di modifica. In particolare, la documentazione può essere presente anche nel codice del programma o in una configurazione.

Dispositivi mobili: dispositivi non vincolati a una posizione geografica e/o dotati di alimentazione mobile (accumulo di energia integrato). I dispositivi mobili tipici sono notebook e smartphone.

3.2 Scopo del marchio di qualità

Il marchio di qualità viene assegnato ai fornitori di servizi informatici che creano e gestiscono l'IT di una PMI. Nel caso di grandi fornitori di servizi IT, solo una parte dell'azienda può ottenere il marchio di qualità. L'ambito deve essere definito dal fornitore di servizi IT. Se il campo di applicazione non riguarda l'intera azienda con tutti i suoi servizi, il campo di applicazione testato viene annotato sul marchio.

3.3 Differenza da altre certificazioni/ Frameworks

Esistono altre certificazioni piuttosto comuni e utili in Svizzera. Nota: CyberSeal è deliberatamente indicato come un marchio di qualità e non come una certificazione. Ciò significa che i requisiti per CyberSeal sono inferiori a quelli richiesti, ad esempio, per la certificazione secondo la norma ISO/IEC 27001

3.3.1 ISO/IEC 27001

Si tratta di uno standard internazionale. In Svizzera il Servizio di accreditamento svizzero SAS, un dipartimento della Confederazione Elvetica, è responsabile dell'implementazione dello standard. In Svizzera, il SAS stabilisce quali società possono effettuare gli audit. Le società accreditate sono elencate sul sito web «Ricerca organismi accreditati SAS (admin.ch)». È comune che un'azienda accreditata da un Paese certifichi anche all'estero.

L'attenzione si concentra piuttosto sulle aziende più grandi. Ciò è dovuto anche al prezzo, poiché la certificazione può essere piuttosto costosa.

Lo standard ha una struttura generica. Ciò consente di mantenere lo standard abbastanza costante. Attualmente è in corso l'audit della versione 2013. Un nuovo standard è attualmente in fase di elaborazione.

Gli sviluppi più recenti (ad esempio, protezione dei dati, cloud computing) sono definiti in standard aggiuntivi. La certificazione secondo questi standard aggiuntivi non è possibile. Tuttavia, essi mostrano come dovrebbe essere interpretato lo standard attuale.

3.3.2 Ragioni per la sicuerezza informatica: BSI (Ufficio federale per la sicurezza informatica)

Il BSI IT-Grundschutz (protezione dei dati IT) è sviluppato e gestito dal BSI tedesco. IT-Grundschutz si basa su oltre 100 elementi costitutivi di IT-Grundschutz (ad esempio, APP 1.2 = browser web, NET.3.2 = firewall). I singoli blocchi sono molto orientati alla pratica e descrivono, ad esempio, una configurazione sicura di un componente. Tuttavia, è molto impegnativo mantenere gli elementi costitutivi ragionevolmente aggiornati.

In Svizzera, il BSI IT-Grundschutz svolge un ruolo importante, soprattutto nell'amministrazione (settore pubblico). Anche molte aziende più grandi tengono conto, almeno in parte, dello standard.

È interessante notare che anche lo standard BSI esiste da tempo. Tuttavia, questo è ampiamente compatibile con gli standard ISO.

3.3.3 Standard minimo delle TIC

Lo standard minimo delle TIC è uno standard svizzero per migliorare la resilienza delle TIC. TIC sta per tecnologie dell'informazione e della comunicazione.

Lo standard è stato emanato dall'Ufficio federale per l'approvvigionamento economico nazionale (UFAE) e si rivolge in particolare ai gestori di infrastrutture sensibili.

Lo standard minimo TIC si basa essenzialmente sul framework NIST.

3.3.4 Ulteriori standard

Esistono molti altri standard, come Cobit e NIST Framework, che svolgono un ruolo subordinato in Svizzera.

4 Aspetti organizzativi dell'Audit

4.1 Lo Standard Cyberseal

Lo standard consiste nel manuale CyberSeal, nella lista di controllo CyberSeal e nel rapporto di audit.

Il manuale di audit dello standard CyberSeal è pubblicato sul sito web digitalsecurityswitzerland.ch. Una versione abbreviata della lista di controllo è disponibile anche sul sito web.

Alleanza Sicurezza Digitale Svizzera ASDS determina il momento in cui la checklist definitiva viene consegnata al fornitore di servizi IT. Occorre tenere presente che la lista di controllo è necessaria per la formazione e il workshop con il fornitore di servizi IT.

I fornitori di servizi IT ricevono il rapporto di audit in forma scritta dopo l'audit CyberSeal.

I punti critici dell'NCSC e delle compagnie di assicurazione devono necessariamente portare a un audit della struttura.

4.2 Grado di conformità ai requisiti di audit

Il marchio di qualità CyberSeal può essere assegnato anche se non tutti i clienti del fornitore di servizi IT soddisfano tutti gli aspetti della sicurezza informatica. Questo può accadere se, ad esempio, il risanamento dei problemi pregressi presso la PMI è costoso o richiede tempo, oppure se il risanamento degli aspetti di sicurezza non è desiderato dalla PMI. Il fornitore di servizi IT deve avvisare questi clienti degli aspetti di sicurezza incompleti almeno una volta all'anno, e il rimedio può richiedere diversi anni.

Il livello di conformità di CyberSeal in questo caso non è del 100%. Il livello minimo di conformità richiesto per ottenere il marchio di qualità CyberSeal è determinato dall'auditor. Il fattore decisivo è che il grado di conformità migliora sensibilmente ogni anno.

4.3 Dichiarazione del fornite di servizi IT

Almeno 10 giorni prima dell'audit, il fornitore di servizi IT deve fornire all'auditor una dichiarazione della lista di controllo CyberSeal completa. Nel caso della "distinzione nel tipo di audit" (vedi capitolo 4.5), le domande dichiarate con autodichiarazione (A) nella lista di controllo vengono affrontate solo in caso di ambiguità. Tuttavia, è importante che tutte le domande (comprese quelle contrassegnate con I (intervista) o C (audit della console) nella lista di controllo) siano risposte al meglio delle proprie conoscenze prima dell'audit.

4.4 Priorità dei requisiti di audit

- Priorità 1: si tratta di requisiti minimi che devono essere implementati. Un'implementazione parziale comporta una non conformità minore che deve essere affrontata entro l'audit successivo. Il trattamento deve portare a un miglioramento significativo del soddisfacimento dei requisiti (cfr. capitolo 4.2 "Grado di conformità ai requisiti di audit").
- Priorità 2: questi requisiti dovrebbero essere soddisfatti da buoni fornitori di servizi IT (best practice). Il mancato adempimento non comporta una divergenza minore. Tuttavia, il revisore può formulare una nota.
- Priorità 3: questo requisito è considerato ragionevole dai professionisti della sicurezza informatica. Nell'ambiente delle PMI, questo requisito non è attualmente considerato obbligatorio.

4.5 Distinzione del tipo di audit

I capitoli die requisiti di audit vengono esaminati in modo diverso:

- Autodichiarazione: di norma, i capitoli non vengono discussi durante l'audit. Si tratta principalmente di capitoli il cui mancato adempimento nell'ambiente delle PMI di solito non comporta danni rilevanti. Spetta al fornitore di servizi IT implementare i dettagli elencati nella lista di controllo. Tuttavia, il revisore può discutere e chiarire singole domande di questi capitoli se le risposte del fornitore di servizi IT non sono da lui comprese.
- Intervista: Anche questi capitoli sono importanti per la cybersecurity delle PMI. L'autodichiarazione compilata viene verificata in sede di audit mediante colloqui.
- Verifica della console: si tratta di capitoli ritenuti molto critici per i danni nell'ambiente delle PMI. Durante l'audit della console, l'auditor effettua un esame concreto dell'implementazione.

4.6 Esclusione dei singoli capitoli

Se singoli capitoli della checklist non hanno senso per un fornitore di servizi (ad esempio, il fornitore di servizi non gestisce una propria infrastruttura di posta elettronica e non la offre ai propri clienti), l'auditore può escludere tali capitoli dall'audit. Il revisore contrassegna questo capitolo come "Non verificabile" (NV) nel campo "Risultato".

4.7 Divergenze

L'auditor utilizza la colonna "Risultato" per valutare il soddisfacimento/non soddisfacimento delle singole domande. A tal fine, utilizza esclusivamente le seguenti abbreviazioni:

- **OK:** Il requisito è sufficientemente soddisfatto

Divergenze
Nel caso di divergenze, si distingue tra:

- **DM (divergenze maggiori):** Questi impediscono l'assegnazione dell'etichetta. Un punto dello standard non è stato rispettato. Le divergenze maggiori sono sempre formulate dall'auditor. Non ci sono grandi divergenze nel capitolo intitolato "autodichiarazione".

In presenza di una o più non conformità gravi, il cliente ha 3 mesi di tempo per porvi rimedio. Dopo questo periodo, l'auditor valuta la correzione della non conformità maggiore.

- **Dm (divergenze minori):** Queste non impediscono l'assegnazione del marchio di qualità. Un punto dello standard è stato attuato solo parzialmente. La divergenza minore deve essere gestita fino alla prossima manutenzione e sarà esaminata in dettaglio nel prossimo audit. Una non conformità al 100% della non conformità minore può essere dichiarata nuovamente come non conformità minore nell'audit successivo. Tuttavia, deve essersi verificato un notevole miglioramento.

- **ND (Note):** Le note sono risultati dell'auditor che possono portare a un miglioramento. Devono essere controllati. Il fornitore di servizi IT decide se e come implementare i risultati.

4.8 Procedura per l'ottenimento del marchio di qualità

Il programma è il seguente:

- Dichiarazione del fornitore di servizi IT.
- Audit per ottenere il sigillo di approvazione, audit rinnovato ogni 3 anni secondo lo standard attuale.
- Audit di manutenzione, ogni anno tra un audit e l'altro.

4.8.1 Preparazione

L'Alleanza Sicurezza Digitale Svizzera (ASDS) offre workshop di orientamento. In questi workshop gratuiti viene spiegata, tra le altre cose, la lista di controllo. Si raccomanda di partecipare a questo workshop. Se il fornitore di servizi IT non vede problemi per l'ottenimento del marchio di qualità (vale a dire che almeno tutti i requisiti della priorità 1 sono sufficientemente soddisfatti per tutti i punti), può registrarsi per l'audit.

4.8.2 Dichiarazione

Il fornitore di servizi IT scarica la lista di controllo. Compila tutte le voci. La dichiarazione compilata fa parte della registrazione. Il foglio di dichiarazione contiene i dati essenziali dell'azienda (numero di dipendenti, settore di attività dell'azienda, ambito definito, strumenti utilizzati, ecc.) La dichiarazione deve essere presentata almeno 10 giorni prima dell'audit.

4.8.3 Audit

Durante l'audit, l'auditor verifica la correttezza dei requisiti di audit con la categoria "Colloquio". I requisiti della categoria "audit della console" devono essere verificati fisicamente, ossia il fornitore di servizi IT deve mostrare l'implementazione concreta. Il controllo di una specifica domanda della lista di controllo è a discrezione dell'auditor. Ad esempio, è possibile esaminare la documentazione e la configurazione degli strumenti corrispondenti. L'audit in loco dura 4 ore. È necessario dedicare almeno 1 ora al "colloquio" e da 2 a 3 ore alla verifica della console. Il revisore impiega circa 4 ore per l'esame preliminare della dichiarazione e l'inserimento delle osservazioni nella lista di controllo. Il marchio di qualità viene concesso se non ci sono gravi non conformità. Eventuali differenze di rilievo devono essere discusse al termine dell'audit. Il cliente deve sapere che non riceverà il certificato.

4.8.4 Audit di manutenzione

Ogni anno, in assenza di audit, deve essere effettuato un audit di manutenzione. L'audit di manutenzione viene eseguito in modo indipendente dal fornitore di servizi IT. Il fornitore di servizi IT descrive tutto il lavoro svolto, che riguarda piccole deviazioni e indicazioni. Questa descrizione da parte del fornitore di servizi IT viene verificata da un auditor e discussa con il fornitore di servizi IT durante una sessione remota. La sessione a distanza dura circa 1 ora e può essere una conversazione telefonica o una videoconferenza

4.9 Costi per l'audit

I costi per l'audit corrispondono ai prezzi aggiornati, che sono indicati su www.digitalsecurityswitzerland.ch.

4.10 Requisiti per l'auditor

L'auditor deve essere un esperto comprovato di sicurezza delle informazioni. Deve conoscere lo sviluppo attuale ed essere in grado di spiegare una corretta implementazione. Deve essere in grado di valutare tecnicamente anche le implementazioni più insolite. La formazione continua dell'esperto deve essere dimostrata.

L'orientamento al cliente e la cordialità del revisore sono importanti.

- La formazione degli auditor si svolge presso la sede di Alleanza Sicurezza Digitale a Zugo. La formazione deve garantire i seguenti obiettivi:
- Gli auditor conoscono in dettaglio i documenti importanti dello standard CyberSeal. Si tratta del Manuale di audit CyberSeal, della Lista di controllo CyberSeal e del Modello di rapporto di audit CyberSeal.
- I revisori conoscono i processi più importanti dell'amministrazione.
- Gli auditor conoscono gli strumenti utilizzati (sito web), i requisiti del computer utilizzato (notebook) e le possibilità di trasferimento sicuro dei dati.
- I revisori effettuano le verifiche nel modo più uniforme possibile.

La formazione vera e propria dei revisori è integrata da corsi di aggiornamento annuali. Nel corso di questa formazione vengono discusse le modifiche allo standard e avviene uno scambio di esperienze tra gli auditor. Anche questo evento può avere un'influenza sullo standard.

Alleanza Sicurezza Digitale Svizzera ASDS è responsabile della nomina dei revisori. Le condizioni sono stabilite da ASDS. Di norma, è auspicabile la partecipazione alla formazione degli auditor. L'ASDS produce anche un documento che regola la formazione degli auditor e ne definisce i costi.

4.11 Svolgimento dell'audit

Se possibile, l'audit viene effettuato fisicamente in loco. Questo aumenta la probabilità di scoprire i punti critici. In casi particolari (periodi di viaggio, pandemia, ecc.), gli audit possono essere eseguiti anche a distanza. Il revisore decide, di concerto con Alleanza Sicurezza Digitale Svizzera, se è possibile effettuare un audit a distanza.

4.12 Sponsorizzazione del marchio di qualità

Lo sponsor del marchio di qualità è Alleanza Sicurezza Digitale Svizzera ASDS. L'ASDS gestisce una filiale (attualmente a Zug) con una corrispondente amministrazione. L'amministrazione ha i seguenti compiti, tra i quali:

- È responsabile dell'ulteriore sviluppo dello standard. L'ASDS può delegare l'ulteriore sviluppo a un gruppo di lavoro. Attualmente esiste un gruppo di lavoro denominato "Audit Committee" che è responsabile dello sviluppo dello standard.
- È Responsabile del sito web con le funzioni appropriate per la registrazione automatica dei fornitori di servizi IT.
- Garantisce il trasferimento sicuro dei dati tra ASDS, revisori e clienti.
- Si assicurai che vengano condotti gli audit (compresi quelli di manutenzione e il nuovo audit CyberSeal dopo tre anni) e che vi sia una comunicazione sufficiente tra i fornitori di servizi IT e gli auditor.
- Mantiene l'elenco degli attuali revisori.
- Coordina e contatta in caso di reclami e opinioni divergenti tra revisori, clienti e ASDS.
- Rilascia il marchio di qualità.
- Marketing e finanza.

4.13 Procedura in caso di pareri discordanti

Se un fornitore di servizi IT dubita del risultato dell'audit, il caso viene valutato da un secondo auditor e viene presa una decisione finale. Il coordinamento del secondo parere viene assunto dall'amministrazione.

Il termine per la presentazione del reclamo è di 30 giorni dal ricevimento del rapporto di revisione.

4.14 Manuale di sicurezza per l'esercizio

Esiste il "Manuale di sicurezza per la gestione della pratica" dell'azienda isec ag. Il manuale di sicurezza è stato sviluppato indipendentemente dallo standard, ma descrive le possibili implementazioni per raggiungere lo standard. Il manuale può essere inteso come una cassetta degli attrezzi. I dettagli sono disponibili sul sito web: https://sihb.ch.

5 **Requisiti per l'audit**

L'audit CyberSeal viene condotto dall'auditor utilizzando la lista di controllo CyberSeal.

Alle singole domande della lista di controllo CyberSeal vengono assegnate delle priorità, come descritto nel capitolo 4.4. Inoltre, la lista di controllo CyberSeal definisce, in conformità con il capitolo 4.5, quali sezioni vengono svolte in autodichiarazione, tramite intervista o audit della console. L'uso della lista di controllo CyberSeal garantisce un'implementazione uniforme degli audit CyberSeal e definisce l'attuale standard CyberSeal.

I contenuti più importanti della lista di controllo CyberSeal sono illustrati di seguito. La formulazione vincolante di ciascun punto di verifica della lista di controllo può essere ricavata.

5.1 Divisione dei compiti tra cliente e fornitore di servizi IT

La divisione dei compiti tra il fornitore di servizi IT e la PMI deve essere messa per iscritto e in modo sufficientemente dettagliato. La documentazione deve

- Descrivete i compiti del fornitore di servizi IT,
- Definire i compiti che il cliente deve svolgere in prima persona.
- Descrivere le responsabilità del fornitore di servizi IT e quelle della PMI.

In particolare, deve essere chiaro chi è responsabile di quali aspetti della sicurezza.

Non è necessario creare un documento separato per ogni cliente. I contratti di manutenzione o le descrizioni dei servizi possono essere sufficienti.

5.2 Gestione dell'accesso all'infrastruttura del cliente

Il fornitore di servizi IT deve dimostrare come regola e gestisce l'accesso all'infrastruttura del cliente.

Devono essere raggiunti i seguenti obiettivi:

- Deve essere garantito che il cliente possa cambiare il fornitore di servizi IT in qualsiasi momento.
- Per l'accesso all'infrastruttura del cliente viene implementato un elevato livello di sicurezza.
- I dipendenti che lasciano un fornitore di servizi IT non hanno più accesso all'infrastruttura del cliente in nessun caso.
- Se si utilizzano le password, queste non devono poter essere ricavate da client diversi. Questo vale in particolare per i conti di servizio.
- Il cliente deve sapere a quali informazioni può accedere il fornitore di servizi IT.

5.3 Documentazione

Il fornitore di servizi IT deve disporre di una documentazione aggiornata dell'infrastruttura della PMI. La documentazione deve comprendere almeno:

- Tutti i sistemi sono elencati in una panoramica.
- La documentazione dei sistemi può essere consegnata al cliente. Non sono necessari sistemi speciali per leggere la documentazione.
- Il fornitore di servizi IT aggiorna regolarmente la documentazione.

5.4 Credenziali e autorizzazioni

Per credenziali si intendono normalmente il nome utente e la password. È necessario assicurarsi che siano soddisfatti i seguenti punti:

- È necessario implementare un processo che tenga traccia di ogni modifica delle credenziali (compresa la reimpostazione della password) e dei permessi. Il processo deve includere anche le autorizzazioni temporanee.
- Il cliente può accedere a tutte le sue credenziali e autorizzazioni in caso di emergenza.
- Le password del cliente sono memorizzate in modo sicuro (ad esempio Passwortsafe).

5.5 Progettazione della rete

La progettazione della rete tiene conto delle diverse zone;

- Zona ufficio
- Zona di produzione, alcuni dispositivi non patchabili possono trovarsi in questa zona.
- Zona pubblica per gli ospiti e dispositivi privati dei dipendenti.

Bisogna fare attenzione che le transizioni tra le zone consentano solo il traffico minimo necessario. In ogni caso, è necessario utilizzare router o dispositivi simili che supportino le regole corrispondenti.

5.6 Firewalls

Devono essere soddisfatte le seguenti condizioni generali:

- Le singole connessioni del firewall consentono solo il traffico necessario. Anche il traffico in uscita verso Internet deve essere limitato.
- Le regole del firewall devono essere leggibili da un esperto esterno.
- Il set di regole deve essere controllato regolarmente. Un controllo effettuato deve essere tracciabile.

5.7 WLAN

La WLAN del fornitore di servizi IT e della PMI si basa fondamentalmente sul concetto del capitolo 5.5. Inoltre, vengono definiti i seguenti requisiti:

- Per ogni cliente devono essere utilizzate password separate e non deteriorabili.
- È necessario predisporre una WLAN separata per i dispositivi privati del personale e per gli ospiti.
- L'autenticazione tramite credenziali condivise può essere utilizzata solo per le zone della rete pubblica. L'accesso a tutte le altre zone (come da capitolo 5.5) deve avvenire esclusivamente con credenziali personali.
- Non vengono utilizzati meccanismi di protezione obsoleti e insicuri (ad es. WEP).

5.8 AD Design

Si garantisce l'attuazione di quanto segue:

- Il cliente può amministrare l'AD autonomamente o incaricare un altro fornitore di servizi di farlo. Ciò può essere garantito dal fatto che il client disponga di un account di amministratore di emergenza.
- Gli account privilegiati non vengono utilizzati per le applicazioni quotidiane. Gli utenti hanno esclusivamente account normali, non privilegiati.
- I portali accessibili al pubblico e le infrastrutture cloud a cui si può accedere tramite le credenziali AD sono implementati in modo sicuro.
- Vengono utilizzati solo account di amministratori personalizzati.

5.9 Protezione dei componenti IT

I sistemi e i dispositivi del cliente configurati dal fornitore di servizi IT sono protetti. In genere, è presente una lista di controllo con le impostazioni necessarie.

5.10 Sistema di posta elettronica

Secondo le informazioni fornite dall'NCSC e dalle compagnie di assicurazione, un attacco informatico inizia con un contatto via e-mail. Pertanto, questo punto è di particolare importanza.

Se il sistema di posta è gestito localmente, si applicano i seguenti requisiti minimi:

- Il sistema di posta elettronica deve essere impostato e gestito in modo sicuro. Oggi è necessario che il sistema di posta elettronica abbia un'ottima protezione anti-malware. Oggi è anche comune che un sistema di posta elettronica controlli l'autenticità del mittente. Questo può essere ottenuto installando SPF o DKIM.

In molti casi, il sistema di posta del cliente viene gestito nel cloud. Con la maggior parte dei provider è possibile garantire un livello di sicurezza molto elevato.

5.11 Gestione delle patch

L'NCSC e le compagnie di assicurazione ritengono che una patch insufficiente e rapida sia la causa di molti attacchi nell'ambiente informatico. Inoltre, a seconda delle vulnerabilità esistenti, queste possono essere utilizzate per ampliare le autorizzazioni. Pertanto, questo punto è di particolare importanza.

I seguenti requisiti devono essere implementati come minimo:

- La gestione delle patch è definita in un processo che deve essere seguito. Il processo comprende anche la gestione delle patch dei prodotti non Microsoft. I cicli di patch sono scelti in modo sensato.
- Le eccezioni alla gestione delle patch (ad esempio, Java per un'applicazione non deve essere patchato) devono essere registrate per iscritto.
- In caso di vulnerabilità gravi e importanti (ad esempio, la vulnerabilità di Exchange), è necessario avviare un processo di emergenza.

5.12 Dispositivi mobili

Attualmente, i dispositivi mobili non sono la causa dei principali incidenti di sicurezza informatica nelle PMI. Tuttavia, è necessario garantire un livello minimo di sicurezza.

- I dati trasportati sui dispositivi mobili devono essere possibilmente criptati.
- L'accesso ai dati aziendali è possibile solo dopo una sufficiente autenticazione.

Molte impostazioni possono essere applicate tecnicamente con i criteri. L'uso di politiche può essere utile ed efficiente per le PMI.

5.13 Home-Office

Molti fornitori di servizi IT possono soddisfare le esigenze dei clienti anche se i loro dipendenti lavorano a casa. Inoltre, l'home office consente di garantire i servizi promessi anche in caso di pandemia.

Pertanto, gli ambienti sicuri per l'home office sono di grande importanza:

- Il fornitore di servizi IT sviluppa un concetto di lavoro sensato e sicuro dall'ufficio di casa e lo implementa.
- Il concetto deve garantire che non sia possibile stabilire una connessione di rete diretta tra i sistemi del cliente e l'home office.
- Deve essere implementata una forma di autenticazione multipla.
- Il concetto descrive anche le funzioni aggiuntive consentite (ad es. stampa, tracciamento delle unità, ecc.).

5.14 ¨Protezione dai malware

Con una buona protezione contro il malware, è possibile prevenire molte contaminazioni. L'NCSC e le compagnie di assicurazione attribuiscono grande importanza a una buona protezione contro il malware. I test condotti in passato hanno dimostrato che esistono grandi differenze tra i numerosi prodotti disponibili sul mercato. Per questo motivo la scelta del prodotto specifico utilizzato è molto importante.

La maggior parte dei server e dei client oggi sono generalmente ben protetti. Molti attacchi avvengono tramite un sistema di posta elettronica. Pertanto, una protezione a due prodotti è obbligatoria per i sistemi di posta elettronica.

È comune, anche nell'ambiente delle PMI, avere una protezione speciale per l'accesso a Internet.

È ancora comune che su alcuni sistemi non sia installata alcuna protezione contro il malware. Il motivo deve essere documentato. Inoltre, tali sistemi devono essere isolati dalla rete.

5.15 Backup

L'NCSC e le compagnie di assicurazione definiscono un buon backup come essenziale per la sopravvivenza di un'azienda in caso di attacco informatico. In caso di attacco informatico, spesso si cerca di rendere inutilizzabile il backup.

Pertanto, un buon backup ha una funzione molto importante. Oltre a una buona documentazione del backup, il suo funzionamento deve essere testato frequentemente. Non solo i singoli file devono essere ripristinati, ma anche interi sistemi devono essere completamente ripristinati e testati per verificarne la funzionalità. Gli attuali ambienti di virtualizzazione e gli strumenti di backup supportano tali test regolari.

Le grandi aziende danno importanza anche al fatto che il backup non possa essere modificato in seguito. Il nastro come supporto di backup sta quindi vivendo un "ritorno". In alternativa, in molti progetti si utilizzano supporti rimovibili. Sono meno sicuri del nastro, ma spesso più economici.

Una copia del backup deve essere conservata in un luogo separato.

5.16 Gestione del cambiamento/gestione degli incidenti

L'argomento è incentrato sulla tracciabilità. Questo può essere importante anche in caso di attacco informatico. Il fornitore di servizi IT garantisce la tracciabilità di tutte le modifiche apportate al sistema. Tutti gli incidenti possono anche essere tracciati.

Questa gestione è talvolta trascurata dai fornitori di servizi IT delle PMI. Tuttavia, non tengono conto del fatto che si può risparmiare molto tempo se un incidente o una modifica possono essere trovati facilmente. Inoltre, i sistemi supportano da soli una gestione primitiva del cambiamento. Tuttavia, è necessario utilizzare questi sistemi in modo coerente.

5.17 Registrazione

Oggi tutti i sistemi supportano un buon logging. Tuttavia, potrebbe essere necessario attivare o configurare questa registrazione. Questo può essere definito con una lista di controllo (si veda anche il capitolo 5.9). È un punto importante di uno SLA. Deve definire il periodo di conservazione e i valori da registrare.

5.18 Monitoraggio

Un buon monitoraggio può essere molto efficiente per un fornitore di servizi IT. Il sistema di monitoraggio può supportare o implementare la gestione del cambiamento. Inoltre, il monitoraggio può rilevare molti attacchi.

Il monitoraggio proattivo può ulteriormente rilevare gli attacchi informatici e supportare la valutazione dei danni.

L'ambito del monitoraggio deve essere definito negli SLA con i clienti. I risultati devono essere regolarmente comunicati al cliente.

5.19 Smaltimento dei supporti di dati

Le informazioni sensibili sono memorizzate su ogni supporto dati. Il fornitore di servizi IT deve garantire che questi dati non cadano in mani non autorizzate. Normalmente, il supporto dati viene distrutto fisicamente.

5.20 Servizi di terze parti

Oggi ogni fornitore di servizi IT deve installare prodotti di terze parti per i clienti. Ad esempio, il cliente può stabilire di lavorare con Office 365 o di utilizzare determinati servizi cloud. Il fornitore di servizi IT conosce questi prodotti e può configurare un livello di sicurezza paragonabile a quello dei servizi locali.

5.21 Vulnerabilità del cliente

Molti clienti utilizzano hardware o software obsoleti e insicuri. Il fornitore di servizi IT ne informa il cliente. È meglio farlo in una conversazione regolare. Si raccomanda vivamente una breve nota di conversazione con le decisioni essenziali.

5.22 Formazione del personale

Questo punto è descritto come molto critico dall'NCSC e dalle compagnie di assicurazione. Gran parte degli attacchi informatici inizia con un'e-mail compromessa. È indispensabile che ogni dipendente sia in grado di riconoscere le e-mail false e di comportarsi correttamente. Pertanto, i clienti e i fornitori di servizi IT devono essere formati regolarmente. Questa formazione comprende anche il comportamento corretto del dipendente quando riceve queste false e-mail.

5.23 Concetto di emergenza

Il NCSC e le compagnie di assicurazione considerano molto importante la preparazione di un concetto di emergenza.

Un concetto di emergenza garantisce che si pensi a tutto in caso di eventi straordinari e che i preparativi necessari possano essere elaborati e testati senza fretta. Il concetto di emergenza deve coprire gli eventi più importanti. Un rischio importante è attualmente rappresentato dalla cibercriminalità (ransomware),

crittografia dei dati, furto di dati e minacce di pubblicazione), che devono essere coperti.

Un'emergenza può verificarsi sia presso il fornitore di servizi IT che presso i clienti di un fornitore di servizi IT. Pertanto, ha senso sviluppare un concetto di emergenza compatibile almeno nell'ambiente informatico. Sarà necessario includere il fornitore di servizi IT nel concetto di emergenza di cliente finale.

Nell'ambiente IT, il concetto di emergenza deve definire chi e come assicura la comunicazione esterna. Inoltre, definisce quali agenzie devono essere informate per risolvere l'emergenza (polizia, NCSC, compagnie di assicurazione, società di supporto, ecc.) Gli indirizzi di contatto corrispondenti fanno parte del concetto di emergenza.

Nell'ambiente IT, la gestione dei dati criptati deve essere regolamentata. Si deve garantire che il recupero dei dati sia possibile anche in caso di guasto dell'AD, ad esempio. È importante effettuare test regolari del concetto di emergenza. Formare le persone chiave e scoprire i punti deboli.

5.24 Date di scadenza

Sono sempre più numerosi i componenti IT che smettono di funzionare dopo una data di scadenza (licenze, certificati, scadenza della manutenzione dei componenti, ecc.) Tutti i componenti che hanno una data di scadenza devono essere monitorati dal fornitore di servizi IT.

Anche l'hardware obsoleto può essere un problema. Se le patch di sicurezza non sono più disponibili, i componenti devono essere sostituiti.

5.25 Sicurezza fisica

La sicurezza fisica deve essere garantita presso la sede del fornitore di servizi IT. L'accesso ai locali del fornitore di servizi IT deve essere regolamentato. In particolare, l'accesso ai centri dati del fornitore di servizi IT deve essere rigorosamente limitato.

Le apparecchiature del fornitore di servizi IT devono essere ragionevolmente protette da influenze esterne (UPS, raffreddamento, connessione internet ridondante, ecc.).

5.26 Gestione dei rischi

Un fornitore di servizi IT deve gestire il rischio in modo significativo. I rischi principali devono essere conosciuti. I rischi possono essere mitigati con le seguenti misure:

- Evitare i rischi: in alcune circostanze, la valutazione dei rischi può portare a non offrire determinati servizi.
- Attenuazione del rischio: vengono adottate misure per attenuare un rischio specifico. Tutti i capitoli precedenti al capitolo 5 sono misure di mitigazione del rischio.
- Trasferimento del rischio: i rischi individuali possono essere assicurati. Il tipo di assicurazione (responsabilità professionale, danni informatici, danni finanziari, ecc.), la somma assicurata e le prestazioni aggiuntive (ad esempio, assistenza in caso di attacco cyber) devono essere scelti con attenzione.

- Accettazione del rischio: ogni azienda deve farsi carico dei singoli rischi (o rischi residui). L'assunzione dei rischi deve essere obbligatoriamente accettata dalla direzione del fornitore di servizi IT e non può essere delegata.

È ragionevole che un fornitore di servizi IT supporti i propri clienti nella creazione di una propria gestione del rischio. A molte domande può rispondere solo il fornitore di servizi IT.

Comitato di revisione di Alleanza Sicurezza Digitale Svizzera

6 Appendice

Elenco delle abbreviazioni

ASDS	Alleanza Sicurezza Digitale Svizzera ASDS
AWS	Amazon Web Service
BSI	Bundesamt für Sicherheit in der Informationstechnik
Cobit	Control Objectives for Information and Related Technology
DKIM	DomainKeys Identified Mail
IEC	International Electrotechnical Commission
IKT	Informations- und Kommunikationstechnik
IPv6	Internet Protocol Version 6
ISO	Internationale Organisation für Normung
PMI	Piccole e medie imprese
NCSC	Centro nazionale per la cibersicurezza
NIST	National Institute of Standards and Technology
SLA	Service Level Agreement
SPF	Sender Policy Framework

Lista di controllo delle abbreviazioni

DM	Divergenze maggiori
Dm	Divergenze minori
NV	Non verificabile
ND	Note
A	Autodichiarazione
I	Intervista
C	Audit della Console