Manuale di revisione CyberSeal

Versione 2.0, 1 maggio 2024

Indice dei contenuti

1 Scopo del documento

Questo manuale descrive in dettaglio l'applicazione della lista di controllo CyberSeal. Descrive inoltre il processo di audit, i costi, le condizioni quadro e altri dettagli relativi all'assegnazione del marchio di qualità CyberSeal. Il manuale viene rivisto annualmente.

2 Il marchio di approvazione CyberSeal

Se l'audit viene superato, Alleanza Sicurezza Digitale Svizzera ASDS assegna 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 siano stati superati gli audit di manutenzione 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) standard e necessarie di oggi. Ciò significa che la sicurezza raggiunta da una PMI dipende in larga misura dal fornitore primario 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 contare sul fatto che un fornitore di servizi IT che ha ottenuto il marchio di qualità CyberSeal tiene sufficientemente conto di importanti aspetti della cibersicurezza.

Durante l'audit CyberSeal, si risponde al catalogo di domande 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 possa essere ottenuto anche dai fornitori di servizi IT più piccoli.

Sono stati presi in considerazione soprattutto gli aspetti della sicurezza che sono fondamentali per le PMI e che sono frequentemente sfruttati da potenziali aggressori nell'ambiente delle PMI. I rapporti delle compagnie di assicurazione e delle organizzazioni governative come UFCS (UFCS, Melani) sui danni effettivi verificatisi nell'ultimo anno sono molto importanti per lo sviluppo dello standard. L'obiettivo è quello di eliminare le vulnerabilità più note e frequentemente sfruttate nelle PMI.

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

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

- Il marchio di qualità tiene conto del radicamento dell'IT nelle PMI svizzere. In particolare, si rivolge alle PMI e ai loro fornitori di servizi IT.
- Il marchio di qualità garantisce che il fornitore di servizi IT adotta le misure di sicurezza più importanti per le PMI standard. L'attenzione è rivolta alla sicurezza informatica.
- Il marchio qualità è molto più facile da ottenere rispetto alla certificazione ISO/IEC 27001.
- Il marchio qualità consente alle PMI di trovare un buon fornitore di servizi IT.
- Il marchio qualità riflette l'attuale situazione di rischio.

3 Nozioni di base

3.1 Termini

Fornitore di servizi IT: il fornitore di servizi IT è un'azienda che fornisce servizi IT a diverse 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 classificate come fornitori di servizi IT.

PMI: una PMI è una piccola o media impresa. Ai fini del marchio di qualità, si presume che una PMI sia piuttosto piccola e che si affidi alle raccomandazioni di un fornitore di servizi IT quando si tratta di sicurezza informatica.

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

Revisore: un revisore nominato dall'organizzazione promotrice Alleanza Sicurezza Digitale Svizzera ASDS, che può assegnare il marchio di qualità. ASDS può anche delegare la nomina dei revisori ad altre società del settore della revisione contabile (ad es. 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 incluse sia le procedure comuni che utilizzano un token (SMS, autenticatore, ecc.) sia altre procedure, 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: sul sito web Proteggere i propri account / password (admin.ch), l'UFCS descrive i requisiti per le password da considerare come autenticazione abbastanza sicura.

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

Dispositivi mobili: dispositivi che non sono legati a una posizione geografica e/o che dispongono di un'alimentazione mobile (accumulo di energia integrato). I dispositivi mobili tipici sono notebook e smartphone.

3.2 Ambito di applicazione del marchio di qualità

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

3.3 Differenziazione da altre certificazioni/quadri

Esistono altre certificazioni piuttosto comuni e utili in Svizzera. Nota: CyberSeal è volutamente indicato come un marchio di qualità e non come una certificazione. Questo per sottolineare che i requisiti per CyberSeal sono inferiori a quelli della certificazione ISO/IEC 27001, ad esempio.

3.3.1 ISO/IEC 27001

Si tratta di uno standard internazionale. In Svizzera, il SAS (Servizio di accreditamento svizzero), un dipartimento del governo federale, è responsabile dell'attuazione dello standard. In Svizzera, il SAS

stabilisce quali aziende sono autorizzate a svolgere gli audit. Le società accreditate sono elencate sul sito web "Ricerca degli organismi accreditati SAS (admin.ch)". È frequente che una società accreditata da un Paese certifichi anche all'estero.

L'attenzione tende a concentrarsi 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. La versione 2022 è attualmente in fase di revisione.

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

3.3.2 Protezione della linea di base IT di BSI

La BSI IT-Grundschutz è sviluppata e gestita dalla BSI tedesca. La protezione di base IT si basa su oltre 100 moduli di protezione di base IT (ad esempio, APP 1.2 = browser web, NET.3.2 = firewall). I singoli moduli sono molto orientati alla pratica e descrivono, ad esempio, la configurazione sicura di un componente. Tuttavia, è molto impegnativo mantenere i moduli ragionevolmente aggiornati.

In Svizzera, la protezione delle basi informatiche BSI riveste un ruolo particolarmente importante nell'amministrazione (settore pubblico). Anche molte grandi aziende tengono conto dello standard, almeno in parte.

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 TIC

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

Lo standard è stato pubblicato dall'Ufficio federale per l'approvvigionamento economico nazionale BWL ed è rivolto in particolare ai gestori di infrastrutture critiche.

Lo standard minimo ICT si basa essenzialmente sul framework NIST.

3.3.4 Ulteriori standard

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

4 Aspetti organizzativi dell'audit

4.1 CyberSeal Standard

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

Il manuale di audit per lo standard CyberSeal è pubblicato sul sito web digitalsecurityswitzerland.ch. Sul sito è disponibile anche una versione ridotta della lista di controllo.

Alleanza Sicurezza Digitale Svizzera ASDS stabilisce il momento in cui la checklist definitiva deve essere presentata al fornitore di servizi IT. Si deve tenere conto del fatto che la checklist è necessaria per la formazione e il workshop con il fornitore di servizi IT.

Dopo l'audit CyberSeal, il rapporto di audit è disponibile per i fornitori di servizi IT online nel loro portale clienti all'indirizzo digitalsecurityswitzerland.ch.

I punti critici di BACS e delle compagnie di assicurazione devono portare a un audit obbligatorio della console.

4.2 Grado di adempimento dei 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, la correzione dei problemi pregressi presso la PMI è costosa o richiede tempo o se la correzione degli aspetti di sicurezza non è desiderata dalla PMI. Il fornitore di servizi IT dovrebbe richiamare l'attenzione di questi clienti sugli aspetti di sicurezza incompleti almeno una volta all'anno, e potrebbero essere necessari diversi anni per correggerli.

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

4.3 Dichiarazione del fornitore 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. Per la "Differenziazione del tipo di audit" (si veda il capitolo 4.5), le domande dichiarate con autodichiarazione (S) nella lista di controllo vengono affrontate solo se non sono chiare. È importante che a tutte le domande (comprese quelle contrassegnate con I (intervista) o C (audit della console) nella lista di controllo) si risponda al meglio delle proprie conoscenze prima dell'audit.

4.4 Priorità ai requisiti di audit

I requisiti di audit sono classificati come segue:

- Priorità 1: Si tratta di requisiti minimi che devono essere implementati. Un'attuazione parziale comporta una deviazione minore che deve essere affrontata nell'audit successivo. Il trattamento deve portare a un miglioramento significativo del soddisfacimento dei requisiti (vedere capitolo 4.2 "Grado di soddisfacimento dei requisiti di audit").
- Priorità 2: Questi requisiti dovrebbero essere soddisfatti da buoni fornitori di servizi IT (best practice). La non conformità non comporta una non conformità minore. Tuttavia, l'auditor può formulare una nota.
- Priorità 3: Questo requisito è considerato ragionevole dagli esperti di sicurezza informatica. Nell'ambiente delle PMI, questo requisito non è attualmente considerato assolutamente necessario.

4.5 Differenziazione del tipo di audit

I capitoli dei requisiti di revisione vengono esaminati in modi diversi:

- **Autodichiarazione**: i capitoli non vengono generalmente discussi durante l'audit. Si tratta principalmente di capitoli il cui mancato rispetto nell'ambiente delle PMI non comporta di solito danni rilevanti. Spetta al fornitore di servizi IT implementare i dettagli elencati nella lista di controllo. Tuttavia, l'auditor può discutere e chiarire le singole domande di questi capitoli se non comprende le risposte del fornitore di servizi IT.
- **Intervista**: Anche questi capitoli sono importanti per la sicurezza informatica delle PMI. L'autodichiarazione compilata viene esaminata durante l'audit mediante interviste.
- **Audit della console**: si tratta di capitoli considerati molto critici per i danni nell'ambiente delle PMI. L'auditor effettua una revisione concreta dell'implementazione durante l'audit della console.

4.6 Esclusione di 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'auditor può escludere questi capitoli dall'audit. L'auditor contrassegna questa sezione 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 solo le seguenti abbreviazioni:

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

Si distingue tra deviazioni:

- **DM (divergenze maggiori)**: Impediscono l'assegnazione del marchio di qualità. Un punto dello standard non è stato rispettato. Le principali non conformità sono sempre formulate dall'auditor. Non ci sono non conformità maggiori nel capitolo "Autodichiarazione".

Se ci sono una o più non conformità principali, il cliente ha 3 mesi di tempo per correggerle. Al termine di questo periodo, l'auditor valuta la correzione della non conformità principale.

- **Dm (divergenze minori)**: Non impediscono l'assegnazione del marchio di qualità. Un punto dello standard è stato implementato solo parzialmente. La deviazione minore deve essere gestita fino alla prossima manutenzione e sarà esaminata in dettaglio durante l'audit successivo. Se la non conformità minore non è stata soddisfatta al 100%, può essere dichiarata nuovamente come non conformità minore nell'audit successivo. Tuttavia, deve aver avuto luogo un miglioramento riconoscibile.

- **ND (note)**: Le note sono i risultati ottenuti dall'auditor che potrebbero portare a un miglioramento. Devono essere controllate. Il fornitore di servizi IT decide se e come implementare le note.

4.8 Procedura per l'ottenimento del marchio di qualità

Il calendario è il seguente:

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

4.8.1 Preparazione

Alleanza Sicurezza Digitale Svizzera ASDS offre workshop di orientamento. In questi workshop gratuiti viene illustrata, tra l'altro, la lista di controllo. Si consiglia di partecipare a questo workshop. Se il fornitore di servizi IT non vede problemi nell'ottenere il marchio di qualità (cioè se 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. 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 della categoria "Colloquio". I requisiti della categoria "Audit su console" devono essere verificati fisicamente, ossia il fornitore di servizi IT deve dimostrare l'effettiva implementazione. Spetta all'auditor decidere come verificare una specifica domanda della lista di controllo. Ad esempio, è possibile esaminare la documentazione e la configurazione degli strumenti pertinenti. L'audit in loco dura 4 ore. Almeno 1 ora deve essere dedicata al "colloquio" e da 2 a 3 ore alla "verifica della console". L'auditor dedica circa 4 ore alla revisione preliminare della dichiarazione e all'inserimento dei commenti nella lista di controllo. Il marchio di qualità viene assegnato se non ci sono gravi non conformità. Le eventuali non conformità maggiori devono essere discusse alla fine dell'audit. Il cliente deve sapere che non riceverà il certificato.

4.8.4 Audit di manutenzione

Nel caso in cui non si effettui alcun audit, è necessario effettuare un audit di manutenzione ogni anno. L'audit di manutenzione viene eseguito in modo indipendente dal fornitore di servizi IT. Il fornitore di servizi IT descrive tutti i lavori svolti che riguardano deviazioni minori e note. Questa descrizione del fornitore di servizi IT viene esaminata da un auditor e discussa con il fornitore di servizi IT durante una sessione remota. La sessione remota dura circa 1 ora e può essere una telefonata o una videoconferenza.

4.9 Costi per gli audit

I costi per l'audit corrispondono ai prezzi attuali, che si possono trovare sul sito www.digitalsecurityswitzerland.ch.

4.10 Requisiti per il revisore

L'auditor deve essere un esperto riconosciuto di sicurezza delle informazioni. Deve conoscere gli sviluppi attuali ed essere in grado di spiegare la corretta implementazione. Deve anche essere in grado di valutare tecnicamente le implementazioni insolite. La formazione continua dell'esperto tecnico deve essere riconosciuta.

L'orientamento al cliente e la cordialità dell'auditor sono importanti.

- La formazione degli auditor si svolge presso la sede di Swiss Digital Security Alliance ADSS 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 amministrativi più importanti.
- Gli auditor conoscono gli strumenti utilizzati (sito web), i requisiti del computer utilizzato (notebook) e le opzioni per il trasferimento sicuro dei dati.
- I revisori effettuano le verifiche nel modo più uniforme possibile.

La formazione vera e propria degli auditor è integrata da un corso di aggiornamento annuale. Durante 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. ASDS stabilisce le condizioni. Di norma, i revisori sono tenuti a partecipare a corsi di formazione. ASDS redige inoltre un documento che regolamenta la formazione degli auditor e ne definisce i costi.

4.11 Esecuzione dell'audit

Ove 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 svolti anche a distanza. L'auditor decide, in accordo con Alleanza Sicurezza Digitale Svizzera ASDS, se l'audit può essere effettuato a distanza.

4.12 Sponsorizzazione del marchio di qualità

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

- Responsabile dell'ulteriore sviluppo dello standard. ASDS può delegare l'ulteriore sviluppo a un gruppo di lavoro. Attualmente esiste un gruppo di lavoro chiamato "Audit Committee", responsabile dello sviluppo dello standard.
- Responsabile del sito web con le relative funzioni per la registrazione automatica dei fornitori di servizi IT.
- Garantire il trasferimento sicuro dei dati tra ASDS, revisori e clienti.
- Assicurarsi che gli audit vengano eseguiti (compresi la 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.
- Mantenere l'elenco degli attuali revisori.
- Coordinamento e referente per i reclami e le opinioni divergenti tra revisori, clienti e ASDS.
- Rilascio del marchio di qualità.
- Marketing e finanza.

4.13 Procedura in caso di opinioni divergenti

Se un fornitore di servizi IT contesta il risultato dell'audit, il caso viene valutato da un secondo revisore e viene presa una decisione finale. Il secondo parere è coordinato dall'amministrazione.

La scadenza per i reclami è di 30 giorni dal ricevimento del rapporto di revisione.

4.14 Manuale di sicurezza per l'uso pratico

Esiste un "Manuale di sicurezza per l'uso pratico" dell'azienda isec ag. Il manuale di sicurezza è stato creato indipendentemente dallo standard, ma descrive le possibili implementazioni per raggiungere lo standard. Il manuale può essere visto come una cassetta degli attrezzi. I dettagli sono disponibili sul seguente sito web: https://sihb.ch.

5 Requisiti di audit

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

Le singole domande della lista di controllo CyberSeal sono classificate in base alla priorità, come descritto nel capitolo 4.4. Inoltre, la lista di controllo CyberSeal, in conformità con il capitolo 4.5, definisce quali sezioni vengono svolte tramite autodichiarazione, intervista o audit su console. L'uso della lista di controllo CyberSeal assicura che gli audit CyberSeal siano eseguiti in modo standardizzato e definisce lo standard CyberSeal attuale.

I contenuti più importanti della lista di controllo CyberSeal sono illustrati di seguito. La formulazione vincolante di ciascun punto di controllo è riportata nella lista di controllo.

5.1 Divisione dei compiti tra cliente e fornitore di servizi IT

La suddivisione dei compiti tra il fornitore di servizi IT e la PMI deve essere descritta per iscritto e in modo

sufficientemente dettagliato. La documentazione deve

- descrivere i compiti del fornitore di servizi IT,
- Definire i compiti che il cliente deve portare a termine da solo.
- 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. Possono essere sufficienti i contratti di manutenzione o le descrizioni dei servizi.

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 (autenticazione multipla). I dipendenti che lasciano un fornitore di servizi IT non hanno più accesso all'infrastruttura del cliente in nessun caso.
- Il cliente deve sapere a quali informazioni può accedere il fornitore di servizi IT.

5.3 Credenziali e autorizzazioni

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

- Deve essere implementato un processo che renda tracciabile ogni modifica delle credenziali (compresa la reimpostazione delle password) e delle autorizzazioni. 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 conservate in modo sicuro (ad esempio, in una cassaforte per password).

5.4 Documentazione

Il fornitore di servizi IT deve disporre di una documentazione aggiornata dell'infrastruttura della PMI. Tale documentazione deve includere 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.

5.5 Progettazione della rete

La progettazione della rete tiene conto delle diverse zone;

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

Si noti che le transizioni tra le zone consentono solo il traffico minimo necessario. In ogni caso, è necessario utilizzare router o dispositivi simili che supportino le regole corrispondenti.

5.6 Firewall

Devono essere soddisfatte le seguenti condizioni:

- 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 rivisto regolarmente. La revisione deve essere tracciabile.

5.7 WLAN

La WLAN presso il fornitore di servizi IT e la PMI si basa fondamentalmente sul concetto di cui alla sezione 5.5. Vengono inoltre definiti i seguenti requisiti:

- Per ogni cliente devono essere utilizzate password separate e non deteriorabili.
- È necessario creare una WLAN separata per i dispositivi privati dei dipendenti 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 (in conformità con la sezione 5.5) deve essere effettuato esclusivamente con credenziali personali.
- Vengono utilizzati solo meccanismi di protezione aggiornati e sicuri.

5.8 Gestione delle identità (Active Directory, Azure, ecc.)

Si assicura che venga attuato quanto segue:

- Il cliente può amministrare l'AD autonomamente o incaricare un altro fornitore di servizi di farlo. Ciò può essere garantito se il cliente dispone di un account di amministratore di emergenza.
- Gli account con autorizzazioni estese non vengono utilizzati per le applicazioni quotidiane.
- I portali accessibili al pubblico e le infrastrutture cloud a cui si può accedere utilizzando le credenziali AD sono implementati in modo sicuro.
- Vengono utilizzati solo account di amministratore personalizzati.

5.9 Protezione dei componenti IT

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

5.10 Sistema di posta elettronica

Secondo l'UFCS e le compagnie di assicurazione, il primo passo di un ciberattacco è un contatto via e-mail. Questo punto è quindi particolarmente importante.

Se l'infrastruttura di posta elettronica è gestita localmente, si applicano i seguenti requisiti minimi:

- L'infrastruttura di posta elettronica deve essere impostata e gestita in modo sicuro. È necessaria una protezione antimalware e la verifica dell'autenticità del mittente, che può essere ottenuta installando SPF o DKIM. L'accesso con i dispositivi mobili viene controllato e limitato di conseguenza.

In molti casi, l'infrastruttura e-mail dei clienti viene gestita nel cloud. La maggior parte dei provider può quindi garantire un livello di sicurezza molto elevato.

5.11 Gestione delle patch

L'insufficienza e la rapidità delle patch sono considerate dalle compagnie BACS e assicurative come la causa di molti attacchi nell'ambiente informatico. Inoltre, a seconda delle vulnerabilità esistenti, queste possono essere utilizzate per estendere le autorizzazioni. Questo punto è quindi di particolare importanza.

Devono essere implementati almeno i seguenti requisiti:

- La gestione delle patch è definita in un processo che deve essere rispettato. Il processo include 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 può essere patchato) devono essere registrate per iscritto.
- In caso di vulnerabilità importanti e gravi (ad esempio, la vulnerabilità di Exchange), è necessario avviare un processo di emergenza.

5.12 Dispositivi mobili

I dispositivi mobili non sono attualmente la causa di gravi incidenti di sicurezza informatica nelle PMI. Tuttavia, è necessario garantire un livello minimo di sicurezza.

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

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

5.13 Lavoro a distanza/ufficio a domicilio

Molti fornitori di servizi IT possono soddisfare le richieste dei clienti anche se i loro dipendenti lavorano da casa. Il lavoro da casa permette anche di garantire i servizi promessi in caso di pandemia.

Gli ambienti sicuri per l'home office sono quindi di grande importanza:

- Il fornitore di servizi IT sviluppa e implementa un concetto di lavoro a distanza sensato e sicuro.
- Questo concetto garantisce che non sia possibile stabilire una connessione di rete diretta tra i sistemi del cliente e l'home office.
- È necessario implementare una forma di autenticazione multipla.
- Il concetto descrive anche le funzioni aggiuntive consentite (ad es. stampa, mappatura delle unità, ecc.).

5.14 Protezione da malware

Molte infezioni possono essere evitate con una buona protezione da malware (protezione da virus). Il BACS e le compagnie di assicurazione attribuiscono grande importanza a una buona protezione da malware. I test condotti in passato hanno dimostrato che esistono notevoli differenze tra i numerosi prodotti disponibili sul mercato. Ciò rende molto importante la scelta del prodotto specifico utilizzato.

La maggior parte dei server e dei client è solitamente ben protetta. Molti attacchi vengono sferrati attraverso un sistema di posta elettronica. Un concetto a due livelli (firewall e client) è quindi essenziale per i sistemi di posta elettronica.

La protezione speciale dell'accesso a Internet è comune, anche nell'ambiente delle PMI.

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

5.15 Backup / Ripristino

Il BACS 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.

Un buon backup ha quindi una funzione molto importante. Oltre a una buona documentazione del backup, è necessario testarne frequentemente la funzionalità. Ciò comporta non solo il ripristino di singoli file, ma anche il ripristino completo di interi sistemi e la verifica della loro funzionalità. Gli attuali ambienti di virtualizzazione e gli strumenti di backup supportano questo tipo di test regolari.

Le grandi aziende attribuiscono inoltre grande importanza alla garanzia che il backup non possa essere modificato in un secondo momento. Il nastro come supporto di backup sta quindi tornando in auge. In alternativa, in molti progetti si utilizzano anche supporti di memorizzazione rimovibili. Questi supporti sono meno sicuri del nastro, ma spesso sono 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 aspetto può essere importante anche in caso di attacco informatico. Il fornitore di servizi IT garantisce la tracciabilità di tutte le modifiche apportate al sistema. Anche tutti gli incidenti possono essere tracciati.

Questa gestione viene talvolta trascurata dai fornitori di servizi IT delle PMI. Tuttavia, ciò non tiene conto del fatto che si può risparmiare molto tempo se un incidente o una modifica possono essere trovati facilmente. I sistemi supportano anche una gestione primitiva delle modifiche. Tuttavia, questi sistemi devono essere utilizzati in modo coerente.

5.17 Registrazione

Ogni sistema supporta una buona registrazione. Tuttavia, potrebbe essere necessario attivare o configurare questa registrazione. Questo può essere fatto 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 delle modifiche. Il monitoraggio può anche rilevare molti attacchi.

Il monitoraggio proattivo può continuare a riconoscere gli attacchi informatici e supportare la valutazione dei danni.

L'ambito del monitoraggio deve essere definito nell'ambito degli SLA con il cliente. I risultati devono essere comunicati regolarmente al cliente.

5.19 Smaltimento dei supporti dati e cancellazione dei dati

Ogni supporto dati contiene informazioni sensibili. Il fornitore di servizi IT deve assicurarsi che questi dati non cadano nelle mani sbagliate. Di norma, il supporto dati viene distrutto fisicamente. Il cliente viene informato dal fornitore di servizi IT dell'obbligo di cancellare regolarmente i dati dai suoi sistemi.

5.20 Servizi di fornitori terzi

Oggi ogni fornitore di servizi IT deve installare prodotti di terze parti per i clienti. Ad esempio, il cliente può decidere 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 Gestire le minacce e le vulnerabilità presso i clienti

Molti clienti utilizzano hardware o software obsoleti e insicuri. Il fornitore di servizi IT richiama l'attenzione del cliente su questo aspetto. Il modo migliore per farlo è un dialogo regolare. Si consiglia di inviare un breve promemoria con le decisioni chiave.

5.22 Formazione dei dipendenti

UFCS e le compagnie di assicurazione considerano questo punto molto critico. Gran parte dei ciberattacchi inizia con un'e-mail compromessa. Ogni dipendente deve essere in grado di riconoscere le e-mail false e di comportarsi correttamente. I clienti e i fornitori di servizi IT devono quindi ricevere una formazione regolare. Questa formazione comprende anche il comportamento corretto del dipendente quando riceve tali e-mail false.

5.23 Piano di emergenza

L'UFCS e le compagnie di assicurazione considerano molto importante la creazione di un piano di emergenza.

Un concetto di emergenza assicura che si pensi a tutto in caso di evento straordinario e che i preparativi necessari possano essere elaborati e testati senza fretta. Il concetto di emergenza deve coprire gli eventi più importanti. La cibercriminalità (ransomware) è attualmente un rischio importante, crittografia dei dati, furto di dati e minaccia di pubblicazione), che devono essere coperti.

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

Nell'ambiente informatico, il concetto di emergenza deve definire chi e come deve essere garantita la comunicazione esterna. Definisce inoltre quali enti devono essere informati per risolvere l'emergenza (polizia, UFCS, compagnie di assicurazione, società di supporto, ecc.) Gli indirizzi di contatto pertinenti fanno parte del concetto di emergenza.

Nell'ambiente IT, la gestione dei dati criptati deve essere regolamentata. Si deve garantire che i dati possano essere recuperati anche in caso di guasto di un AD, ad esempio. I test regolari del concetto di emergenza sono importanti. Essi addestrano il personale chiave e mettono in luce 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, procedure di manutenzione dei componenti, ecc.) Tutti i componenti che hanno una data di scadenza devono essere monitorati dal fornitore di servizi IT.

L'hardware obsoleto rappresenta un ulteriore rischio. Se le patch di sicurezza non sono più disponibili, i componenti devono essere sostituiti.

5.25 Sicurezza fisica

La sicurezza fisica deve essere garantita dal 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 ridotto al minimo.

I dispositivi del fornitore di servizi IT devono essere protetti in modo adeguato contro le influenze esterne (UPS, raffreddamento, connessione Internet ridondante, ecc.).

5.26 Gestione del rischio

Un fornitore di servizi IT deve adottare un sistema di gestione del rischio ragionevole. I rischi principali devono essere noti. I rischi possono essere ridotti al minimo con le seguenti misure:

- Evitare i rischi: in alcune circostanze, la valutazione dei rischi può comportare l'impossibilità di offrire determinati servizi.
- Riduzione del rischio: vengono adottate misure per ridurre al minimo un rischio specifico. Tutti i capitoli precedenti della sezione 5 sono misure di minimizzazione del rischio.
- Trasferimento del rischio: è possibile assicurare i singoli rischi. Il tipo di assicurazione (responsabilità civile professionale, danni informatici, perdite finanziarie, ecc.), la somma assicurata e le prestazioni aggiuntive (ad esempio, assistenza in caso di attacco informatico) devono essere scelti con attenzione.
- Accettazione dei rischi: ogni azienda deve assumersi i singoli rischi (o rischi residui). L'assunzione dei rischi deve essere accettata dal management del fornitore di servizi IT e non può essere

delegata.

Un fornitore di servizi IT dovrebbe supportare i propri clienti nella creazione del proprio sistema di gestione del rischio. Un fornitore di servizi IT può aiutarli in molti casi e rispondere alle loro domande.

Comitato dei revisori di Allenza Sicurezza Digitale Svizzera.

6 Appendice

Elenco delle abbreviazioni

ASDS	Alleanza Sicurezza Digitale Svizzera
UFCS	Ufficio federale della cibersicurezza
BSI	Ufficio federale per la sicurezza delle informazioni
Cobit	Control Objectives for Information and Related Technology
DKIM	DomainKeys Identified Mail
IEC	Commissione Elettrotecnica Internazionale
TIC	Tecnologia dell'informazione e della comunicazione
ISO	Organizzazione internazionale per la normazione
PMI	Piccole e medie imprese
NCSC	National Cyber Security Center
NIST	Istituto Nazionale di Standardizzazione e Tecnologia
SLA	Service Level Agreement
SPF	Sender Policy Framewor

Lista di controllo delle abbreviazioni

DM Divergenze maggiori

Dm Divergenze minori

NV Non verificabile

ND Nota

IC Infrastruttura del cliente

IP Infrastruttura propria / infrastruttura del fornitore di servizi IT

A Autodichiarazione

I Intervista

C Audit della Console