CyberSeal - Lista di controllo

Cap.	Pg.	Controllo	Prio	Metodo dell'Audit A=Autodichiarazione I=Intervista C=Console	Infra-struttura propria	Infra-struttura del cliente
5.1		**Condivisione dei compiti cliente/fornitore di servizi IT**				
	1	Esiste un accordo scritto sulla divisione dei compiti/responsabilità con tutti i clienti (ad esempio, uno SLA, un contratto di manutenzione, una descrizione del servizio).	1	I	x	x
5.2		**Gestione dell'accesso all'infrastruttura del cliente**				
	1	Le modifiche del personale presso il fornitore di servizi IT possono essere implementate facilmente. Un ex dipendente non può più accedere al sito del cliente	1	I	x	
	2	Il cliente non può accedere alle risorse del fornitore di servizi IT o di altri clienti.	1	I	x	x
	3	Per ogni cliente si usano password diverse.	1	I		x
	4	L'accesso all'infrastruttura client è possibile solo con dispositivi protetti. I jumphost e le macchine virtuali sono considerati controllati.	1	I		x
	5	Tutti i clienti sono a conoscenza della portata delle autorizzazioni del fornitore di servizi IT.	1	I		x
	6	L'accesso all'infrastruttura del cliente deve essere sicuro (ad es. autenticazione a più fattori). L'accesso non autorizzato da parte di terzi deve essere impedito il più possibile.	1	I		x
	7	Per un account tecnico, è necessario utilizzare una password forte.	2	I	x	x
5.3		**Documentazione**				
	1	Per ogni client, è disponibile una documentazione generale con almeno il nome dell'host, l'indirizzo IP e lo scopo del componente gestito.	1	I		x
	2	La documentazione può essere consegnata al cliente su richiesta (in formato elettronico comunemente utilizzato, come PDF o cartaceo).	1	I		x
	3	La documentazione è aggiornata (non più vecchia di 1 mese).	2	I	x	x
5.4		**Credenziali e autorizzazioni**				
	1	Ogni modifica degli account (comprese le password) o delle autorizzazioni è tracciabile.	1	A	x	x
	2	In caso di emergenza, le password sono accessibili.	1	A	x	x
	3	Esiste un processo definito e sicuro per la modifica di account, password e autorizzazioni.	2	A	x	x
	4	Esiste un processo definito e sicuro per le autorizzazioni temporanee.	2	A	x	x
	5	Le password del cliente sono tenute al sicuro (password safe o simili).	2	A		x
5.5		**Progettazione della rete**				
	1	La rete è segmentata: ad esempio, rete dell'ufficio, rete in funzione (componenti non patchabili), WLAN, WLAN guest.	1	A	x	x
	2	I collegamenti tra le zone hanno una connettività minima (ad esempio, tramite firewall).	2	A	x	x
5.6		**Firewalls**				
	1	Le regole devono essere leggibili (denominazioni significative che corrispondono alla documentazione). È auspicabile una documentazione nel manuale.	1	I	x	x
	2	L'insieme di regole è definito nel modo più ristretto possibile. Ad esempio, le regole Any-Any non sono consentite, il traffico in uscita è limitato. Le eccezioni devono essere giustificate.	2	I	x	x
	3	Il regolamento deve essere rivisto periodicamente e in modo comprensibile. Si raccomanda un principio di controllo doppio.	2	I	x	x
5.7		**WLAN**				
	1	Per ogni cliente devono essere utilizzate password separate e non falsificabili.	1	I	x	x
	2	È necessario predisporre una WLAN separata per i dispositivi privati del personale e per gli ospiti.	1	I	x	x
	3	Nella zona ufficio, ogni dipendente ha il proprio account. In altre zone sono ammessi account generici.	2	I	x	x
	4	Non vengono utilizzati meccanismi di protezione obsoleti o insicuri.	2	I	x	x
5.8		**AD Design**				
	1	Il cliente dispone di un account amministratore di emergenza.	1	A		x
	2	Gli account con autorizzazioni estese non vengono utilizzati per le operazioni di applicazione quotidiana.	2	A	x	x
	3	I portali accessibili al pubblico (ad esempio Azure) sincronizzati con il proprio AD sono protetti con l'autenticazione a più fattori.	2	A	x	x
	4	Il fornitore di servizi IT dispone di un proprio account di amministratore su tutti i sistemi client.	2	A	x	x
5.9		**Protezione dei componenti IT**				
	1	Il fornitore di servizi IT dispone di un processo definito e sicuro per l'hardening dei sistemi (client, server, componenti di rete).	1	I	x	x
5.10	**KR**	**Sistema di posta elettronica**				
	1	Il fornitore di servizi IT garantisce che le infrastrutture di posta elettronica siano protette da malware e spam.	1	C	x	x
	2	Il fornitore di servizi IT supporta solo infrastrutture di posta che controllano l'autenticità del mittente (SPF, DKIM, ecc.).	1	C	x	x
	3	L'accesso con i telefoni cellulari ai sistemi di posta elettronica è consentito solo con una politica tecnicamente restrittiva adattata alle esigenze dell'azienda.	1	C	*x*	*x*
5.11	**KR**	**Gestione delle patch**				
	1	Il fornitore di servizi IT dispone di un processo definito e sicuro per l'applicazione delle patch.	1	C	x	x
	2	Il fornitore di servizi IT assicura che tutti i sistemi e le applicazioni rilevanti siano patchati, oltre al sistema operativo Microsoft anche altre applicazioni (ad esempio ERP e Adobe), sistemi in produzione, firewall e dispositivi di rete. Le eccezioni giustificate vengono registrate per iscritto.	2	C	x	x
	3	Nella zona ufficio vengono utilizzati solo i sistemi (sistemi operativi) che ricevono ancora le patch di sistema.	2	C	x	x
	4	Viene utilizzato uno strumento per il patching centralizzato dei client. Il sistema di patch è automatizzato e centralizzato.	2	C	x	x
5.12		**Dispositivi mobili (laptop, tablet, smartphone)**				
	1	I supporti di dati sui sistemi mobili sono criptati.	1	I	x	x
	2	L'accesso ai dati aziendali è possibile solo dopo una sufficiente autenticazione.	1	I	x	x
	3	Esistono requisiti per i dispositivi mobili. I requisiti sono applicati dalle politiche.	2	I	x	x
5.13		**Home Office**				
	1	L'accesso dall'ufficio di casa è possibile solo tramite i sistemi controllati (l'accesso dai dispositivi BYOD è possibile solo tramite desktop virtuali).	1	I	x	x

CyberSeal - Lista di controllo

Cap.	Pg.	Controllo	Prio	Metodo dell'Audit A=Autodichiarazione I=Intervista C=Console	Infra-struttura propria	Infra-struttura del cliente
	2	L'accesso dalla sede centrale è possibile solo dopo l'autenticazione a due fattori. I dispositivi protetti sono considerati un fattore se l'accesso è possibile solo con i dispositivi controllati.	1	I	x	x
	3	Altri servizi sono consentiti solo con Home Office dopo un controllo di sicurezza (ad es. stampa e mappatura delle unità).	2	I	x	x
5.14	**KR**	**Protezione da malware**				
	1	Tutti i dispositivi sono dotati di protezione contro il malware, a condizione che i dispositivi lo consentano tecnicamente. Il sistema di whitelisting delle applicazioni e dei servizi è considerato come una protezione contro i malware	1	C	x	x
	2	Viene implementato un concetto a due livelli (firewall e client).	1	C	x	x
	3	I sistemi senza protezione da malware (ad esempio i sistemi di produzione) devono essere isolati dalla rete.	2	C	x	x
5.15	**KR**	**Backup/Ripristino**				
	1	Il fornitore di servizi IT dispone di un processo definito e sicuro per il backup/ripristino dei sistemi e dei servizi necessari (ad es. server, componenti di rete, servizi cloud).	1	C	x	x
	2	Il backup viene testato regolarmente. Sono necessari regolari test di ripristino di interi sistemi (server), compresi i dati.	1	C	x	x
	3	Una copia di backup di sicurezza deve essere mantenuta localmente separata.	1	C	x	x
	4	L'accesso in scrittura ai dati di backup non è più possibile dopo il backup. Si consiglia un backup offline (nastro, supporto rimovibile).	2	C	x	x
5.16		**Change Management / Incident Management**				
	1	Tutte le modifiche ai sistemi sono registrate in modo tracciabile.	2	A	x	x
	2	Tutti gli incidenti rilevanti possono essere tracciati.	2	A	x	x
5.17		**Procedura**				
	1	Il fornitore di servizi IT deve garantire che tutti i registri di sistema siano conservati in conformità con l'accordo (si raccomanda lo SLA).	1	A		x
	2	Bisogna registrare almeno ogni accesso del fornitore di servizi IT ai sistemi del cliente e i guasti all'hardware.	1	A		x
	3	Il protocollo deve essere conservato per almeno 6 mesi.	2	A		x
5.18		**Monitoraggio**				
	1	Il fornitore di servizi IT deve monitorare i sistemi del cliente e, se necessario, adottare misure adeguate.	2	A		x
5.19		**Smaltimento dei supporti di dati**				
	1	Il fornitore di servizi IT dispone di un processo definito e sicuro per lo smaltimento dei supporti di dati.	1	A	x	x
	2	Esiste una procedura per la cancellazione dei dati.	2	I	x	
	3	Il fornitore di servizi IT offre ai propri clienti una consulenza sulla cancellazione dei dati.	3	A		x
5.20		**Servizi di terze parti**				
	1	Il fornitore di servizi IT conosce i prodotti di terze parti che supporta e può offrire un livello di sicurezza paragonabile a quello dei servizi locali.	2	I		x
	2	Il fornitore di servizi IT si assicura che i suoi clienti ricevano regolarmente rapporti sui servizi forniti e sulla disponibilità del fornitore terzo. Il cliente viene inoltre informato delle modifiche alle certificazioni.	3	A	x	
5.21		**Gestire le minacce e le vulnerabilità dei clienti**				
	1	Il fornitore di servizi IT informa i clienti sulle possibili minacce e vulnerabilità dell'infrastruttura o dei servizi gestiti.	2	A		x
5.22	**KR**	**Formazione del personale**				
	1	Il fornitore di servizi IT offre ai propri clienti una formazione di sensibilizzazione (ad esempio, incentrata sull'ingegneria sociale) o indirizza i propri clienti a un fornitore di tali corsi.	2	C		x
	2	Il fornitore di servizi IT organizza regolarmente corsi di formazione per i propri dipendenti sul tema della sicurezza informatica (con particolare attenzione all'ingegneria sociale).	1	C	x	
5.23	**KR**	**Concetto di emergenza**				
	1	Esiste un concetto di emergenza aggiornato e specifico per l'azienda. Il sistema tiene conto anche di ricatti, fughe di dati e crittografia dei dati.	1	C	x	x
	2	Il concetto di emergenza regola anche il coinvolgimento di agenzie esterne (polizia, NCSC, compagnie di assicurazione, società di supporto, ecc.)	2	C	x	x
	3	Il fornitore di servizi IT offre ai suoi clienti un supporto per la creazione di un concetto di emergenza.	2	A	x	x
	4	Il concetto di emergenza è aggiornato e viene testato in modo appropriato.	2	C	x	x
5.24		**Date di scadenza**				
	1	Vengono conservate le date di scadenza dei componenti informatici (ad es. certificati, licenze, ecc.). Un messaggio viene generato automaticamente in tempo utile prima della scadenza.	2	A	x	x
	2	L'attenzione del cliente è rivolta all'hardware e al software obsoleti e ai rischi associati.	2	A	x	x
5.25		**Sicurezza fisica**				
	1	L'accesso ai locali del fornitore di servizi IT è controllato e ragionevolmente limitato.	1	I	x	
	2	L'accesso al centro dati del fornitore di servizi IT deve essere autorizzato e registrato.	2	I		
	3	Le apparecchiature informatiche del fornitore di servizi sono protette da influenze esterne (ad es. USV, raffreddamento, connessione internet ridondante).	2	I	x	
5.26		**Gestione dei rischi informatici**				
	1	Ogni anno viene effettuata una gestione del rischio informatico/analisi del rischio. Il VR firma il Rapporto sul rischio informatico all'attenzione del GL, accettando così i rischi residui.	2	I	x	
	2	È stato stabilito un processo per mitigare i rischi informatici.	2	I	x	
	3	È stato esaminato un ragionevole trasferimento dei rischi informatici a una compagnia assicurativa.	2	I	x	
	4	Se necessario, il fornitore di servizi IT supporta il cliente nelle questioni di gestione del rischi informatici.	3	I		x