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 con tutti i clienti (ad esempio, uno SLA, un contratto di manutenzione, una descrizione del servizio).	1	I	x	x
	2	Esiste una persona/ruolo responsabile della cibersicurezza	1	I	x	
	3	Il fornitore di servizi IT deve fornire al cliente un rapporto periodico sulla sicurezza.	2	I	x	
5.2		**Gestione dell'accesso all'infrastruttura del cliente**				
	1	I cambiamenti di personale presso il fornitore di servizi IT possono essere facilmente implementati. Un ex dipendente non può più accedere all'infrastruttura/dati 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	L'accesso all'infrastruttura del cliente è possibile solo con dispositivi gestiti. I jumphost e i computer virtuali sono considerati gestiti.	1	I		x
	4	Tutti i clienti sono a conoscenza della portata delle autorizzazioni del fornitore di servizi IT.	1	I		x
	5	Per accedere all'infrastruttura del cliente è necessaria l'autenticazione a più fattori.	1	I		x
	6	L'accesso all'infrastruttura del cliente viene registrato.	2	I	x	
5.3		**Credenziali e autorizzazioni**				
	1	Ogni modifica agli account (comprese le password) o alle autorizzazioni è tracciabile.	1	A	x	x
	2	Le password del cliente sono forti, uniche e conservate in modo sicuro (cassaforte per password o simili).	1	A	x	
	3	Le password sono accessibili in caso di emergenza.	1	A	x	x
	4	Gli account privilegiati devono essere particolarmente protetti.	1	A	x	x
	5	Esiste un processo definito e sicuro per la mutazione di account, password e autorizzazioni.	2	A	x	x
	6	Esiste un processo definito e sicuro per le autorizzazioni temporanee.	2	A	x	x
5.4		**Documentazione**				
	1	Per ogni cliente è disponibile una panoramica con almeno il nome dell'host, l'indirizzo IP e lo scopo dei componenti gestiti (inventario).	1	I		x
	2	La documentazione può essere fornita al cliente su richiesta (generalmente in formato elettronico come PDF o cartaceo).	1	I		x
	3	La documentazione è aggiornata (non più vecchia di 1 mese dall'ultima modifica).	2	I	x	x
5.5		**Progettazione della rete**				
	1	La rete è segmentata: ad esempio, rete dell'ufficio, componenti centrali (storage, piattaforma di virtualizzazione, componenti di rete), rete in produzione, WLAN, WLAN guest.	1	A	x	x
	2	I sistemi/applicazioni non patchabili devono essere gestiti in una rete separata.	1	A	x	x
	3	Le transizioni tra le zone hanno una connettività minima (ad esempio, utilizzando 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 set di regole.	1	I	x	x
	2	Il set di regole deve essere rivisto regolarmente e in modo comprensibile. Si raccomanda un principio di doppio controllo.	1	I	x	x
	3	Il set di regole è definito nel modo più restrittivo possibile. Ad esempio, le regole any-any non sono consentite e anche il traffico in uscita è limitato. Le eccezioni devono essere giustificate.	2	I	x	x
5.7		**WLAN**				
	1	Per ogni cliente devono essere utilizzate password separate e non deteriorabili.	1	I	x	x
	2	È necessario creare una WLAN separata per i dispositivi privati dei dipendenti e per gli ospiti.	1	I	x	x
	3	I certificati vengono utilizzati per l'autenticazione nella zona ufficio.	2	I	x	x
	4	Vengono utilizzati solo meccanismi di protezione aggiornati e sicuri.	2	I	x	x
5.8		**Gestione delle identità (Active Directory, Azure, ...)**				
	1	Il cliente dispone di un account di amministratore di emergenza, a meno che non vi rinunci esplicitamente.	1	A		x
	2	Gli account con autorizzazioni estese non vengono utilizzati per le applicazioni quotidiane.	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 dei clienti.	2	A	x	x
	5	Le identità e le autorizzazioni devono essere controllate regolarmente (almeno ogni anno).	2	A	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		**Mail-System**				
	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 elettronica che controllano l'autenticità del mittente (SPF, DKIM, ecc.).	1	C	x	x
	3	L'accesso ai sistemi di posta elettronica con dispositivi mobili è consentito solo con una politica aziendale personalizzata e tecnicamente restrittiva.	1	C	*x*	*x*
5.11		**Patch-Management**				
	1	Il fornitore di servizi IT dispone di un processo definito e sicuro per l'applicazione delle patch.	1	C	x	x
	2	Le patch vengono eseguite con una cadenza ragionevole.	1	C	x	x
	3	Il fornitore di servizi IT garantisce che tutti i sistemi e le applicazioni pertinenti siano sottoposti a patch, compresi i sistemi operativi, le applicazioni/app, i sistemi di produzione, i firewall e i dispositivi di rete. Le eccezioni giustificate vengono registrate per iscritto.	2	C	x	x
	4	Deve essere possibile reagire immediatamente ai punti deboli più importanti e conosciuti.	2	C	x	x
	5	Il sistema di patch per i clienti è automatizzato e centralizzato.	2	C	x	x
5.12		**Mobile Devices (Laptops, Tablets, Smartphones)**				
	1	I supporti o i contenitori 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
	4	Viene utilizzata la gestione dei dispositivi o delle applicazioni.	3	A	x	x
5.13		**Remote Work / Home Office**				

CyberSeal - Lista di controllo

Cap.	Pg.	Controllo	Prio	Metodo dell'Audit A=Autodichiarazione I=Intervista C=Console	Infra-struttura propria	Infra-struttura del cliente
	1	L'accesso al lavoro a distanza è possibile solo tramite sistemi gestiti (ad esempio, l'accesso da dispositivi BYOD solo tramite desktop virtuali).	1	I	x	x
	2	L'accesso al lavoro remoto è possibile solo dopo l'autenticazione a più fattori.	1	I	x	x
	3	È stata concordata con i dipendenti una politica di lavoro a distanza.	2	I	x	
5.14		**Malware-Protection**				
	1	Tutti i sistemi sono dotati di protezione da malware, nella misura in cui ciò è tecnicamente possibile.	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	I	x	x
	4	È in uso una soluzione di rilevamento e risposta degli endpoint.	3	A	x	x
5.15		**Backup / Restore**				
	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 test regolari di ripristino di interi sistemi (server), compresi i dati.	1	C	x	x
	3	Una copia di backup sufficiente è costituita da più generazioni e deve essere conservata separatamente e in modo inalterabile.	1	C	x	x
	4	L'infrastruttura di backup non è accessibile tramite la normale gestione delle identità.	2	I	x	x
5.16		**Change Management / Incident Management**				
	1	Tutte le modifiche ai sistemi critici del fornitore di servizi vengono effettuate secondo processi definiti e sono registrate in modo tracciabile.	1	A	x	
	2	Tutte le modifiche ai sistemi dei clienti sono registrate in modo tracciabile.	2	A		x
	3	Tutti gli incidenti rilevanti per la sicurezza vengono gestiti secondo un processo definito e possono essere tracciati.	2	A	x	x
5.17		**Registrazione**				
	1	Il fornitore di servizi IT si assicura che tutti i log di sistema siano archiviati in conformità con l'accordo (si raccomanda lo SLA).	1	A		x
	2	Almeno ogni accesso del fornitore di servizi IT ai sistemi del cliente e gli errori hardware devono essere registrati.	1	A		x
5.18		**Monitoraggio**				
	1	Il fornitore di servizi informatici monitora i sistemi e, se necessario, adotta misure adeguate.	2	A	x	x
	2	I sistemi di sicurezza sono monitorati. Gli allarmi vengono gestiti.	3	A	x	x
5.19		**Smaltimento dei supporti dati / cancellazione dei dati**				
	1	Il fornitore di servizi IT dispone di un processo definito e sicuro per lo smaltimento dei supporti dati.	1	A	x	x
	2	Esiste un processo di cancellazione dei dati	2	A	x	
5.20		**Servizi di fornitori terzi**				
	1	Il fornitore di servizi IT conosce i prodotti gestiti da fornitori terzi e può offrire un livello di sicurezza paragonabile a quello dei servizi locali.	2	A		x
	2	Il fornitore di servizi IT si assicura che i suoi clienti ricevano regolarmente rapporti sui servizi forniti e sulla disponibilità di fornitori terzi.	3	A	x	
5.21		**Gestire le minacce e le vulnerabilità presso i clienti**				
	1	Il fornitore di servizi IT informa i clienti sulle potenziali minacce e vulnerabilità dell'infrastruttura o dei servizi che supporta.	2	A		x
	2	Esiste un sistema di gestione delle vulnerabilità.	3	A	x	x
5.22		**Formazione per i dipendenti**				
	1	Viene definita e applicata una politica per gli utenti e l'amministrazione (ad esempio, una politica di utilizzo accettabile).	1	C	x	
	2	Il fornitore di servizi informatici organizza regolarmente corsi di formazione sulla sicurezza delle informazioni per i propri dipendenti.	1	C	x	
	3	Il fornitore di servizi IT offre ai propri clienti servizi di sensibilizzazione o li indirizza a un fornitore terzo.	2	A		x
5.23		**Concetto di emergenza**				
	1	È stato predisposto un concetto di emergenza aggiornato, disponibile in caso di emergenza. Tra le altre cose, tiene conto della crittografia e della divulgazione dei dati, nonché del ricatto.	1	C	x	x
	2	Il concetto di emergenza viene testato in modo appropriato e regolare.	2	A	x	x
	3	Il concetto di emergenza regola anche il coinvolgimento di organizzazioni esterne (polizia, BACS, compagnie assicurative, società di supporto, ecc.).	2	A	x	x
	4	Il fornitore di servizi IT offre ai suoi clienti un supporto per l'elaborazione di un moderno concetto di emergenza.	2	A	x	x
5.24		**Date di scadenza**				
	1	Vengono registrate le date di scadenza dei componenti IT (ad esempio, certificati, licenze, ecc.). Viene generato un messaggio in tempo utile prima della scadenza.	2	A	x	x
	2	L'attenzione del cliente è rivolta all'hardware e al software obsoleti, con i relativi rischi.	2	A	x	x
5.25		**Sicurezza fisica**				
	1	L'accesso ai locali del fornitore di servizi IT è controllato e sensibilmente limitato.	1	I	x	
	2	L'accesso al centro dati del fornitore di servizi IT deve essere autorizzato e registrato.	1	I		
	3	Le apparecchiature informatiche del fornitore di servizi sono protette da influenze esterne (ad es. UPS, raffreddamento, connessione Internet ridondante).	2	I	x	
5.26		**Gestione del rischio IT**				
	1	Ogni anno viene effettuata una gestione/analisi dei rischi. Il CdA firma il rapporto sui rischi all'attenzione dell'MB, accettando così i rischi residui.	2	I	x	
	2	È stato stabilito un processo per affrontare i rischi inaccettabili.	2	I	x	
	3	Il fornitore di servizi IT supporta il cliente nelle questioni di gestione del rischio, come richiesto.	3	A		x