Version 1.5, Date: 15.05.2023

CyberSeal - Liste des points de contrôle

Chap.	Pt.	Contrôle	Prio	AET	PI	IC
5.1		**Répartition des tâches client/prestataire IT**				
	1	Il existe un accord écrit sur la répartition des tâches et des responsabilités avec tous les clients (par ex. un SLA, un contrat de maintenance, une description de service).	1	E	x	x
5.2		**Gestion de l'accès à l'infrastructure du client**				
	1	Les changements de personnel au sein du prestataire IT peuvent être facilement mis en œuvre. Un ancien collaborateur ne peut plus ouvrir de session chez un client.	1	E	x	
	2	Le client ne peut pas accéder aux ressources du prestataire IT ou à celles d'autres clients.	1	E	x	x
	3	Des mots de passe différents sont utilisés pour chaque client.	1	E		x
	4	L'accès à l'infrastructure du client n'est possible que depuis des appareils gérés. Les «jumphosts» et les ordinateurs virtuels sont considérés comme étant gérés.	1	E		x
	5	Tous les clients ont conscience de l'étendue des autorisations du prestataire IT.	1	E		x
	6	Une authentification à plusieurs facteurs est nécessaire pour accéder à l'infrastructure du client.	1	E		x
	7	Pour un compte technique, il faut utiliser un mot de passe fort.	2	E	x	x
5.3		**Documentation**				
	1	Une documentation récapitulative est établie pour chaque client comprend au moins le nom d'hôte, l'adresse IP et le but des composants gérés.	1	E		x
	2	Sur demande, la documentation peut être remise au client (dans un format électronique généralement répandu comme le PDF ou sur papier).	1	E		x
	3	La documentation est actuelle (pas plus d'un mois)	2	E	x	x
5.4		**Identifiants et Autorisations**				
	1	Toutes les modifications de comptes (y compris les mots de passe) ou d'autorisations sont traçables ou disposent d'un fichier de type log.	1	A	x	x
	2	Les mots de passe sont accessible en cas d'urgence.	1	A	x	x
	3	Il existe un processus défini et sécurisé pour les modifications de comptes, de mots de passe et d'autorisations.	2	A	x	x
	4	Il existe un processus défini et sécurisé pour les autorisations temporaires.	2	A	x	x
	5	Les mots de passe du client sont conservés en toute sécurité (coffre-fort numérique).	2	A		x
5.5		**Structure du réseau**				
	1	Le réseau est segmenté: p. ex., réseau bureautique, Production (composants pour lesquels il n'existe aucun correctif), WLAN, WLAN visiteurs	1	A	x	x
	2	Les transitions entre les zones ont une connectivité minimale (p. ex., par le biais de pare-feux)	2	A	x	x
5.6		**Pare-feux**				
	1	Les règles doivent être lisibles (désignations sensées et conformes à la documentation). Documentation souhaitée de la gestion de règles	1	E	x	x
	2	La gestion des règles doit être définie le plus étroitement possible. P. ex., interdiction de règles any-any, limitation du trafic sortant. Les exceptions doivent être justifiées.	2	E	x	x
	3	La gestion des règles doit être régulièrement contrôlée de manière compréhensible. Il est recommandé d'appliquer le principe du double contrôle.	2	E	x	x
5.7		**WLAN**				
	1	Des mots de passe distincts et non déductibles doivent être utilisés pour chaque client.	1	E	x	x
	2	Mise en place d'un réseau WLAN séparé pour les appareils privés des collaborateurs et pour les visiteurs	1	E	x	x
	3	Tous les collaborateurs disposent de leur propre compte dans la zone bureautique. Des comptes génériques sont autorisés dans les autres zones.	2	E	x	x
	4	Aucun mécanisme de protection obsolète ou peu sûr n'est utilisé.	2	E	x	x
5.8		**Active Directory Design**				
	1	Le client dispose d'un compte administrateur de secours.	1	A		x
	2	Les comptes disposant d'autorisations étendues ne sont pas utilisés pour les travaux d'applications quotidiens.	2	A	x	x
	3	Les portails accessibles au public (p. ex., Azure) et synchronisés avec leur propre AD sont protégés par une authentification à facteurs multiples.	2	A	x	x
	4	Le prestataire de services informatiques dispose de son propre compte d'administrateur sur tous les systèmes du client.	2	A	x	x
5.9		**Durcissement des composants informatiques**				
	1	Le prestataire de services informatiques dispose d'un processus défini et sécurisé pour le durcissement des systèmes (clients, serveurs, composants réseau).	1	E	x	x
5.10	**KR**	**Système de messagerie**				
	1	Le prestataire IT s'assure que les infrastructures de messagerie sont protégées contre les malwares et les spams.	1	T	x	x
	2	Le prestataire de services informatiques ne prend en charge que les infrastructures de messagerie qui vérifient l'authenticité de l'expéditeur (SPF. DKIM, etc.).	1	T	x	x
	3	L'accès aux systèmes de messagerie électronique par téléphone portable n'est autorisé qu'avec une politique techniquement restrictive et adaptée aux besoins de l'entreprise.	1	T	*x*	*x*
5.11	**KR**	**Gestion des correctifs**				
	1	Le prestataire IT dispose d'un processus défini et sûr pour l'importation de correctifs	1	T	x	x
	2	Le prestataire de services informatiques s'assure que tous les systèmes et applications pertinents sont patchés, non seulement Microsoft OS mais aussi d'autres applications (par ex. ERP et Adobe), les systèmes dans la production, le pare-feu et les appareils de réseau. Les exceptions justifiées sont consignées par écrit.	2	T	x	x
	3	Les systèmes utilisés dans la zone Office (systèmes opérationnels) sont uniquement des systèmes recevant des correctifs.	2	T	x	x
	4	Un outil est utilisé pour le patch client centralisé. Le système de patch est automatisé et centralisé.	2	T	x	x
5.12		**Dispositifs mobiles (ordinateurs portables, tablettes, smartphones)**				
	1	Les supports de données sur les appareils mobiles sont chiffrés.	1	E	x	x
	2	L'accès aux données de l'entreprise n'est possible qu'après une authentification suffisante.	1	E	x	x
	3	Des exigences pour les dispositifs mobiles sont définies. Ces exigences sont appliquées par l'intermédiaire de directives.	2	E	x	x
5.13		**Télétravail**				
	1	L'accès en télétravail n'est autorisé que par des systèmes gérés (accès d'appareils BYOD uniquement par des ordinateurs virtuels)	1	E	x	x

CyberSeal - Liste des points de contrôle

Chap.	Pt.	Contrôle	Prio	AET	PI	IC
	2	L'accès en télétravail n'est possible qu'après une authentification à deux facteurs. Lorsque l'accès n'est possible qu'avec des appareils gérés, ceux-ci sont considérés comme un facteur.	1	E	x	x
	3	Certains services supplémentaires ne sont autorisés en télétravail qu'après une vérification de sécurité (p. ex., problèmes d'imprimante, mappage de lecteur autorisé sur les appareils gérés).	2	E	x	x
5.14	**KR**	**Protection contre les logiciels malveillants**				
	1	Tous les appareils sont dotés d'une protection contre les logiciels malveillants, pour autant que les appareils le permettent techniquement. Le whitelisting des apps et des services est considéré comme une protection contre les malwares. Protection contre les logiciels malveillant	1	T	x	x
	2	Un concept à deux niveaux (pare-feu et client) est mis en œuvre.	1	T	x	x
	3	Les systèmes sans protection contre les malwares (p. ex., systèmes de production) doivent être isolés du réseau.	2	T	x	x
5.15	**KR**	**Sauvegarde/Restauration**				
	1	Le prestataire de services informatiques dispose d'un processus défini et sécurisé pour la sauvegarde/restauration des systèmes et services nécessaires (par ex. : serveurs, composants réseau, services cloud).	1	T	x	x
	2	La sauvegarde est régulièrement testée. Il est nécessaire de tester régulièrement les restaurations de l'ensemble des systèmes (serveurs), y compris les données.	1	T	x	x
	3	Une copie de sauvegarde suffisante doit être conservée séparément (géographiquement).	1	T	x	x
	4	Un accès en écriture à la sauvegarde n'est plus possible après la sauvegarde. Il est recommandé d'effectuer une sauvegarde hors ligne (bande, support de données amovible)	2	T	x	x
5.16		**Gestion des modifications / Gestion des incidents**				
	1	Toutes les modifications effectuées sur les systèmes font l'objet d'un procès-verbal et sont traçables.	2	A	x	x
	2	Tous les incidents sont traçables.	2	A	x	x
5.17		**Procès-verbaux**				
	1	Le prestataire IT s'assure que tous les procès-verbaux du système sont conservés conformément à l'accord (SLA recommandé).	1	A		x
	2	Il faut consigner au moins tous les accès du prestataire IT à l'infrastructure du client et les pannes de hardware.	1	A		x
	3	Les procès-verbaux sont conservés pendant au moins 6 mois.	2	A		x
5.18		**Suivi**				
	1	Le prestataire de services informatiques effectue un monitoring des systèmes du client et prend les mesures appropriées si nécessaire.	2	A		x
5.19		**Élimination de supports de données**				
	1	Le prestataire de services informatiques dispose d'un processus défini et sécurisé pour l'élimination des supports de données.	1	A	x	x
	2	Il existe un processus de suppression des données.	2	E	x	
	3	Le prestataire de services informatiques offre à ses clients des conseils sur la suppression des données.	3	A		x
5.20		**Services de fournisseurs tiers**				
	1	Le prestataire de services informatiques connaît les produits tiers dont il s'occupe et peut offrir un niveau de sécurité comparable à celui des services locaux.	2	E		x
	2	Le fournisseur de services informatiques veille à ce que ses clients reçoivent régulièrement des rapports sur les prestations fournies et sur la disponibilité des fournisseurs tiers. Les modifications concernant les certifications sont également communiquées au client.	3	A	x	
5.21		**Gestion des menaces et des vulnérabilités chez les clients**				
	1	Le prestataire de services informatiques informe les clients des menaces et des vulnérabilités potentielles de l'infrastructure ou des services qu'il gère.	2	A		x
5.22	**KR**	**Formation des collaborateurs**				
	1	Le prestataire de services informatiques propose à ses clients des formations de sensibilisation (par ex. axées sur l'ingénierie sociale) ou met ses clients en contact avec un prestataire de tels cours.	2	T		x
	2	Le prestataire IT organise régulièrement des formations pour ses collaborateurs sur le thème de la sécurité informatique (en mettant l'accent sur l'ingénierie sociale).	1	T	x	
5.23	**KR**	**Plan d'urgence**				
	1	Un concept d'urgence spécifique à l'entreprise et actualisé est disponible. Il tient compte, entre autres, du chantage, de la fuite de données et du cryptage des données.	1	T	x	x
	2	Le concept d'urgence règle également l'implication des services externes (police, NCSC, assurances, entreprises de soutien, etc.).	2	T	x	x
	3	Le prestataire de services informatiques propose à ses clients une assistance pour l'élaboration d'un plan d'urgence	2	A	x	x
	4	Le concept d'urgence est à jour et testé de manière appropriée.	2	T	x	x
5.24		**Éléments arrivant à échéance**				
	1	Les données relatives à l'échéance des composants informatiques sont gérées (p. ex., certificats, licences, etc.). Une notification automatique est générée avant l'échéance	2	A	x	x
	2	Le client est rendu attentif à l'obsolescence du matériel et des logiciels, ainsi qu'aux risques qui y sont liés.	2	A	x	x
5.25		**Sécurité physique**				
	1	L'accès aux locaux du prestataire de services informatiques est contrôlé et judicieusement limité.	1	E	x	
	2	Une autorisation de la direction est nécessaire pour accéder au centre de données du prestataire IT et elle doit être consignée.	2	E		
	3	Les appareils informatiques du prestataire de services sont protégés contre les influences extérieures (par ex. onduleur, refroidissement, connexion Internet redondante).	2	E	x	
5.26		**Gestion des risques IT**				
	1	Une gestion des risques informatiques / une analyse des risques est effectuée chaque année. Le CA signe le rapport sur les risques informatiques à l'attention de la direction et accepte ainsi les risques restants.	2	E	x	
	2	Un processus de réduction des risques est établi.	2	E	x	
	3	Un transfert sensé de risques IT à une compagnie d'assurance a été vérifié.	2	E	x	
	4	Si besoin est, le prestataire IT soutient le client concernant les questions de gestion de risques IT	3	E		x