Version 2.0, date : 01.05.2024

CyberSeal
Liste des points de contrôle

Cap.	Pt.	Contrôle	Prio	Mèthode dâudit: A=Autodèclaration E=Entretien T=Terminaux (console)	Propre infra-structure	Infra-structure du client
5.1		**Répartition des tâches client/fournisseur de services informatiques**				
	1	Il existe un accord écrit sur la répartition des tâches avec tous les clients (par ex. un SLA, un contrat de maintenance, une description de service).	1	E	x	x
	2	Il existe une personne/un rôle responsable de la cybersécurité.	1	E	x	
	3	Le prestataire de services informatiques établit un rapport de sécurité régulier à l'intention du client.	2	E	x	
5.2		**Gestion de l'accès à l'infrastructure du client**				
	1	Les mutations de personnel chez le prestataire de services informatiques peuvent être facilement mises en œuvre. Un ancien employé ne peut plus accéder à l'infrastructure/aux données du client.	1	E	x	
	2	Le client ne peut pas accéder aux ressources chez le prestataire de services informatiques ou chez d'autres clients.	1	E	x	x
	3	L'accès à l'infrastructure du client n'est possible qu'avec des appareils gérés. Les jumphosts et les ordinateurs virtuels sont considérés comme gérés.	1	E		x
	4	Tous les clients sont conscients de l'étendue des autorisations du prestataire de services informatiques.	1	E		x
	5	Une authentification à plusieurs facteurs est nécessaire pour accéder à l'infrastructure du client.	1	E		x
	6	Les accès à l'infrastructure du client sont consignés.	2	E	x	
5.3		**Crédentiels et autorisations**				
	1	Toute mutation des comptes (y compris des mots de passe) ou des autorisations est traçable.	1	A	x	x
	2	Les mots de passe du client sont forts, uniques et conservés en toute sécurité (coffre-fort pour mots de passe ou autre).	1	A	x	
	3	En cas d'urgence, les mots de passe sont accessibles.	1	A	x	x
	4	Les comptes privilégiés doivent être particulièrement bien sécurisés.	1	A	x	x
	5	Il existe un processus défini et sécurisé pour la mutation des comptes, du mot de passe et des autorisations.	2	A	x	x
	6	Il existe un processus défini et sécurisé pour les autorisations temporaires.	2	A	x	x
5.4		**Documentation**				
	1	Pour chaque client, il existe une documentation récapitulative comprenant au moins le nom d'hôte, l'adresse IP et le but des composants gérés (inventaire).	1	E		x
	2	La documentation peut être remise au client sur demande (format électronique généralement répandu comme le PDF ou le papier).	1	E		x
	3	La documentation est à jour (pas plus d'un mois après la dernière modification).	2	E	x	x
5.5		**Conception du réseau**				
	1	Le réseau est segmenté : par exemple réseau de bureau, composants de base (stockage, plateforme de virtualisation, composants réseau), réseau dans la production, WLAN, WLAN pour les invités.	1	A	x	x
	2	Les systèmes/applications non patchables doivent être exploités sur un réseau séparé.	1	A	x	x
	3	Les transitions entre les zones ont une connectivité minimale (par exemple au moyen de pare-feux).	2	A	x	x
5.6		**Pare-feux**				
	1	Les règles doivent être lisibles (désignations pertinentes et conformes à la documentation). La documentation dans le Ruleset est souhaitée.	1	E	x	x
	2	Le Ruleset doit être contrôlé régulièrement et de manière compréhensible. Un principe de double contrôle est recommandé.	1	E	x	x
	3	Le jeu de règles est défini le plus étroitement possible. Par exemple, les règles any-any ne sont pas autorisées, le trafic sortant est également limité. Les exceptions doivent être justifiées.	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	Un réseau WLAN séparé doit être mis en place pour les appareils privés des collaborateurs et pour les invités.	1	E	x	x
	3	Dans la zone Office, l'authentification s'effectue à l'aide de certificats.	2	E	x	x
	4	Seuls des mécanismes de protection actuels et sûrs sont utilisés.	2	E	x	x
5.8		**Gestion des identités (Active Directory, Azure, ...)**				
	1	Le client possède un compte d'administrateur de secours, sauf s'il y renonce explicitement.	1	A		x
	2	Les comptes dotés d'autorisations étendues ne sont pas utilisés pour les travaux d'application quotidiens.	2	A	x	x
	3	Les portails accessibles au public (p. ex. Azure) qui sont synchronisés avec le 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	Les identités et les autorisations doivent être vérifiées régulièrement (au moins une fois par an).	2	A	x	
5.9		**Hardening 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		**Système de messagerie**				
	1	Le prestataire de services informatiques s'assure que les infrastructures de messagerie sont protégées contre les logiciels malveillants et le spam.	1	T	x	x

CyberSeal
Liste des points de contrôle

Cap.	Pt.	Contrôle	Prio	Mèthode dâudit: A=Autodèclaration E=Entretien T=Terminaux (console)	Propre infra-structure	Infra-structure du client
	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 avec des appareils mobiles n'est autorisé qu'avec une Company Policy adaptée et techniquement restrictive de l'entreprise.	1	T	x	x
5.11		**Gestion des correctifs**				
	1	Le prestataire de services informatiques dispose d'un processus défini et sécurisé pour l'application des correctifs.	1	T	x	x
	2	Le patching se fait à une cadence raisonnable.	1	T	x	x
	3	Le prestataire de services informatiques s'assure que tous les systèmes et applications pertinents sont patchés, non seulement les systèmes d'exploitation, mais aussi les applications, les systèmes de production, les pare-feu et les appareils de réseau. Les exceptions justifiées sont consignées par écrit.	2	T	x	x
	4	En cas de points faibles importants et connus, il faut pouvoir réagir immédiatement.	2	T	x	x
	5	Le système de patchs pour les clients est automatisé et centralisé.	2	T	x	x
5.12		**Appareils mobiles (ordinateurs portables, tablettes, smartphones)**				
	1	Les supports de données ou les conteneurs sur les systèmes mobiles sont cryptés.	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	Il existe des exigences pour les appareils mobiles. Ces exigences sont appliquées par des politiques.	2	E	x	x
	4	Une gestion des périphériques ou des applications est mise en place.	3	A	x	x
5.13		**Travail à distance / Bureau à domicile**				
	1	L'accès au travail à distance n'est possible que via des systèmes gérés (par exemple, l'accès aux appareils BYOD n'est possible que via des bureaux virtuels).	1	E	x	x
	2	L'accès à Remote Work n'est possible qu'après une authentification à plusieurs facteurs.	1	E	x	x
	3	Une politique de travail à distance est convenue avec les collaborateurs.	2	E	x	
5.14		**Protection contre les logiciels malveillants**				
	1	Tous les systèmes sont dotés d'une protection contre les logiciels malveillants, dans la mesure où ils le permettent techniquement.	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 logiciels malveillants (par ex. les systèmes de production) doivent être isolés au niveau du réseau.	2	E	x	x
	4	Une solution Endpoint Detection and Responce est en place.	3	A	x	x
5.15		**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. Des tests de restauration de l'ensemble des systèmes (serveurs), y compris les données, sont nécessaires à intervalles réguliers.	1	T	x	x
	3	Une copie de sauvegarde suffisante se compose de plusieurs générations, doit être conservée séparément sur le plan local et ne doit pas être modifiée.	1	T	x	x
	4	L'accès à l'infrastructure de sauvegarde ne se fait pas via la gestion régulière des identités.	2	E	x	x
5.16		**Gestion du changement / gestion des incidents**				
	1	Toutes les modifications des systèmes critiques du prestataire de services sont effectuées selon des processus définis et sont consignées de manière compréhensible.	1	A	x	
	2	Toutes les modifications apportées aux systèmes des clients sont consignées de manière compréhensible.	2	A		x
	3	Tous les incidents liés à la sécurité sont traités selon un processus défini et peuvent être suivis.	2	A	x	x
5.17		**Consignation des données**				
	1	Le prestataire de services informatiques s'assure que tous les journaux du système sont conservés conformément à l'accord (SLA recommandé).	1	A		x
	2	Au moins chaque accès du prestataire de services informatiques aux systèmes du client et les pannes de matériel doivent être consignés.	1	A		x
5.18		**Suivi**				
	1	Le prestataire de services informatiques effectue un monitoring des systèmes et prend les mesures appropriées si nécessaire.	2	A	x	x
	2	Les systèmes de sécurité sont surveillés. Les alarmes sont traitées.	3	A	x	x
5.19		**Élimination des supports de données / Effacement des 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	A	x	
5.20		**Services de 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	A		x
	2	Le responsable des services informatiques veille à ce que ses clients reçoivent régulièrement un rapport sur les prestations fournies et sur les disponibilités des fournisseurs tiers.	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
	2	Une gestion des points faibles est effectuée.	3	A	x	x
5.22		**Formation du personnel**				

CyberSeal
Liste des points de contrôle

Cap.	Pt.	Contrôle	Prio	Mèthode dâudit: A=Autodèclaration E=Entretien T=Terminaux (console)	Propre infra-structure	Infra-structure du client
	1	Une politique d'utilisation et d'administration (par ex. Acceptable Use Policy) est définie et appliquée.	1	T	x	
	2	Le prestataire de services informatiques organise régulièrement des formations sur le thème de la sécurité de l'information pour ses propres collaborateurs.	1	T	x	
	3	Le prestataire de services informatiques propose des services de sensibilisation à ses clients ou les met en relation avec un prestataire tiers.	2	A		x
5.23		**Concept d'urgence**				
	1	Un concept d'urgence actuel est en place et disponible en cas d'urgence. Il tient compte entre autres du cryptage et de la divulgation des données, ainsi que du chantage.	1	T	x	x
	2	Le concept d'urgence est testé de manière appropriée et régulière.	2	A	x	x
	3	Le concept d'urgence règle également l'implication des services externes (police, BACS, assurances, entreprises de soutien, etc.).	2	A	x	x
	4	Le prestataire de services informatiques propose à ses clients de les aider à mettre en place un plan d'urgence moderne.	2	A	x	x
5.24		**Dates d'expiration**				
	1	Les dates d'expiration des composants informatiques (p. ex. certificats, licences, etc.) sont gérées. Un message est généré à temps avant l'expiration.	2	A	x	x
	2	Le client est rendu attentif à l'obsolescence du matériel et des logiciels, y compris aux risques qui y sont liés.	2	A	x	x