Manuel d'audit du CyberSeal

Version 2.0, 01.05.2024

Table des matières

1 Objectif du document 4
2 Le label de qualité CyberSeal 4
3 Principes de base 5
3.1 Termes 5
3.2 Portée du label de qualité 5
3.3 Délimitation par rapport à d'autres certifications/cadres 6
4 Aspects organisationnels de l'audit 7
4.1 CyberSeal Standard 7
4.2 Degré de conformité aux exigences de l'audit 7
4.3 Déclaration par le prestataire de services informatiques 7
4.4 Priorisation des exigences d'audit 7
4.5 Distinction dans le type d'examen 8
4.6 Exclusion de certains chapitres 8
4.7 Divergences 8
4.8 Déroulement pour l'obtention du label de qualité 9
4.9 Coûts des audits 9
4.10 Exigences envers l'auditeur 10
4.11 Réalisation de l'audit 10
4.12 Organisme responsable du label de qualité 10
4.13 Procédure en cas d'avis divergents 11
4.14 Manuel de sécurité pour la pratique 11
5 Exigences en matière d'audit 11
5.1 Répartition des tâches client/prestataire informatique 11
5.2 Gestion de l'accès à l'infrastructure du client 11
5.3 Crédentiels et autorisations 12
5.4 Documentation 12
5.5 Conception du réseau 12
5.6 Pare-feu 12
5.7 WLAN 12
5.8 Gestion des identités (Active Directory, Azure, etc.) 13
5.9 Hardening des composants informatiques 13
5.10 Système de messagerie 13
5.11 Gestion des correctifs 13
5.12 Appareils mobiles 14
5.13 Travail à distance / bureau à domicile 14
5.14 Protection contre les logiciels malveillants 14

5.15 Sauvegarde / Restauration 14
5.16 Gestion du changement/gestion des incidents 15
5.17 Consignation des données 15
5.18 Suivi 15
5.19 Élimination des supports de données & Effacement des données 15
5.20 Services de tiers 15
5.21 Gestion des menaces et des vulnérabilités chez les clients 15
5.22 Formation du personnel 16
5.23 Concept d'urgence 16
5.24 Dates d'expiration 16
5.25 Sécurité physique 16
5.26 Gestion des risques 17
6 Annexe 18

1 Objectif du document

Ce manuel décrit en détail l'utilisation de la liste de contrôle CyberSeal. Il décrit en outre le processus d'audit, les coûts, les conditions générales et d'autres détails concernant l'attribution du label de qualité CyberSeal. Le manuel est révisé chaque année.

2 Le label de qualité CyberSeal

En cas de réussite de l'audit, l'Alliance pour la sécurité numérique en Suisse ADSS décerne au prestataire de services informatiques le label de qualité CyberSeal. Ce label de qualité confirme que le prestataire de services informatiques a réussi l'audit sans écart majeur.

Le label de qualité est valable trois ans à condition que les audits de maintien soient réussis les deux et trois années suivantes.

Le label de qualité CyberSeal se base sur le fait que la grande majorité des PME travaillent en étroite collaboration avec un prestataire de services informatiques primaire, car une PME n'est généralement pas en mesure d'assurer les aspects d'une mise en place et d'une exploitation sûres des technologies de l'information (TI) courantes et nécessaires aujourd'hui. Ainsi, la sécurité atteinte par une PME dépend en grande partie du prestataire de services informatiques primaire. Le label de qualité permet de définir les aspects de sécurité que le prestataire de services informatiques doit mettre en œuvre pour lui-même et pour ses clients. La PME peut être sûre qu'un prestataire de services informatiques ayant reçu le label de qualité CyberSeal tient suffisamment compte des aspects importants de la cybersécurité.

Lors de l'audit CyberSeal, il est répondu à la liste de questions de la liste de contrôle CyberSeal. Les questions sont classées par ordre de pertinence. La catégorisation a été choisie de manière à ce que le label de qualité soit également accessible aux petits fournisseurs de services informatiques.

On tient compte en premier lieu des aspects de sécurité qui sont centraux pour les PME et qui sont souvent exploités par des agresseurs potentiels dans l'environnement des PME. Pour le développement de la norme, les déclarations des assurances et des organisations gouvernementales telles que BACS (NCSC, Melani) sur les dommages effectivement survenus l'année dernière sont très importantes. L'objectif est de remédier aux vulnérabilités les plus connues et les plus souvent exploitées par les PME.

Le label de qualité CyberSeal est très exigeant en matière d'actualité. Les derniers développements en matière d'agresseurs et de types de dommages sont intégrés chaque année dans la norme adaptée.

Le label de qualité CyberSeal se distingue à plusieurs égards des labels, labels de qualité et certifications de sécurité de l'information courants (comme ISO/CEI 27001) :

- Le label de qualité tient compte de l'intégration de l'informatique dans les PME suisses. Il s'adresse en particulier aux PME et à leurs prestataires de services informatiques.
- Le label de qualité garantit que le prestataire de services informatiques prend les mesures de sécurité les plus pertinentes pour les PME habituelles. L'accent est mis sur la cybersécurité.
- Le label de qualité est beaucoup plus facile à obtenir qu'une certification ISO/IEC 27001.
- Le label de qualité permet aux PME de trouver un bon prestataire de services informatiques.
- Le label de qualité reflète la situation actuelle en matière de risques.

3 Principes de base

3.1 Termes

Fournisseur de services informatiques : le fournisseur de services informatiques est une entreprise qui fournit des services informatiques à différentes PME. Le prestataire de services informatiques est donc également le point de confiance central en ce qui concerne la sécurité informatique des PME. Il y a environ 5 000 entreprises en Suisse qui sont considérées comme des fournisseurs de services informatiques.

PME : une PME est une petite ou moyenne entreprise. Pour le label de qualité, on part du principe qu'une PME est plutôt petite et qu'elle s'appuie sur les recommandations d'un prestataire de services informatiques pour les questions de sécurité informatique.

Prestataires de services tiers : Autres prestataires de services mandatés par le prestataire de services informatiques ou la PME pour fournir des prestations ou des services. Le prestataire de services informatiques est responsable de l'intégration sécurisée de ce fournisseur tiers. Les fournisseurs tiers peuvent être très différents : Fournisseurs d'applications (par ex. Abacus), Dropbox, Office 365 et autres fournisseurs de cloud.

Auditeur : un auditeur désigné par l'organisation responsable Alliance pour la sécurité numérique en Suisse ADSS, qui peut attribuer le label de qualité. L'ADSS peut également déléguer la nomination d'auditeurs à d'autres entreprises dans le domaine de l'audit (p. ex. BDO, etc.).

Compte à privilèges : Un compte qui dispose de droits élevés sur le système, la configuration et/ou l'écriture.

Authentification multifactorielle : deux facteurs différents sont généralement utilisés pour l'authentification. Dans le présent document, cela inclut les procédures courantes utilisant un jeton (SMS, Authenticator, etc.) ainsi que d'autres procédures telles que les plages d'adresses IP restreintes et les appareils protégés par certificat.
Les authentifications nécessaires à plusieurs reprises (par exemple, un login système suivi d'un login d'application ne sont pas considérées comme des authentifications à plusieurs facteurs).

Mots de passe forts : l'OFPC décrit sur la page web Protégez vos comptes / Mots de passe (admin.ch) les conditions pour que les mots de passe puissent être considérés comme une authentification assez sûre.

Documentation : une documentation est toute forme d'information qui peut être trouvée, qui est compréhensible, qui est contrôlée périodiquement et qui est soumise à une procédure de modification. Une documentation peut notamment être présente dans le code du programme ou dans une configuration.

Appareils mobiles : appareils qui ne sont pas liés à un emplacement géographique et/ou qui possèdent une alimentation électrique mobile (stockage d'énergie intégré). Les ordinateurs portables et les smartphones sont des appareils mobiles typiques.

3.2 Portée du label de qualité

Le label de qualité est attribué aux prestataires de services informatiques qui mettent en place et gèrent l'informatique d'une PME. Pour les prestataires de services informatiques plus importants, seul un secteur de l'entreprise est éventuellement doté d'un label de qualité. Le champ d'application doit être défini par le prestataire de services informatiques. Si le champ d'application ne concerne pas l'ensemble de l'entreprise avec tous ses services, le champ d'application contrôlé est mentionné sur le label.

3.3 Délimitation par rapport à d'autres certifications/cadres

Il existe d'autres certifications qui sont tout à fait courantes et utiles en Suisse. Remarque : dans le cas du CyberSeal, on parle délibérément d'un label de qualité et non d'une certification. Cela signifie que les exigences du CyberSeal sont moins élevées que celles d'une certification ISO/IEC 27001 par exemple.

3.3.1 ISO/IEC 27001

Il s'agit d'une norme internationale. En Suisse, le SAS (Service d'accréditation suisse), un département de la Confédération, est chargé de la mise en œuvre de la norme. En Suisse, le SAS détermine quelles entreprises peuvent effectuer des audits. Les entreprises accréditées sont listées sur le site web "Recherche d'organismes accrédités SAS (admin.ch)". Il est courant pour une entreprise accréditée par un pays d'être également certifiée à l'étranger.

L'accent est plutôt mis sur les grandes entreprises. Cela s'explique aussi par le prix, car une certification peut être assez coûteuse.

La norme est conçue de manière générique. Cela permet de maintenir la norme à un niveau constant. Actuellement, les audits sont effectués selon la version de l'année 2022.

Les développements plus récents (par exemple la protection des données, le cloud computing) sont définis dans des normes supplémentaires. Une certification selon ces normes supplémentaires n'est pas possible. Elles indiquent toutefois comment la norme proprement dite doit être interprétée.

3.3.2 BSI Protection IT de base

La protection informatique de base BSI est élaborée et maintenue par le BSI allemand. La protection IT de base se base sur plus de 100 modules IT de base (par ex. APP 1.2 = navigateur web, NET.3.2 = pare-feu). Les différentes briques sont très orientées vers la pratique et décrivent par exemple une configuration sûre d'un composant. Il est toutefois très difficile de maintenir les blocs de construction à jour dans une certaine mesure.

En Suisse, le BSI-IT-Grundschutz joue un rôle important, surtout dans l'administration (secteur public). De nombreuses grandes entreprises tiennent également compte de cette norme, du moins en partie.

Il est intéressant de noter qu'il existe en outre depuis quelque temps la norme BSI. Or, celle-ci est largement compatible avec les normes ISO.

3.3.3 Norme minimale TIC

La norme minimale TIC est une norme suisse visant à améliorer la résilience des TIC. TIC signifie technologies de l'information et de la communication.

La norme a été publiée par l'Office fédéral pour l'approvisionnement économique du pays OFAE et s'adresse en particulier aux exploitants d'infrastructures critiques.

La norme minimale en matière de TIC est essentiellement basée sur le cadre du NIST.

3.3.4 Autres normes

Il existe de nombreux autres standards comme Cobit, NIST-Framework, qui jouent un rôle secondaire en Suisse.

4 Aspects organisationnels de l'audit

4.1 CyberSeal Standard

La norme se compose du manuel CyberSeal, de la liste de contrôle CyberSeal et du rapport d'audit.

Le manuel d'audit de la norme CyberSeal est publié sur le site digitalsecurityswitzerland.ch. De même, une version abrégée de la liste d'audit est disponible sur le site.

Alliance pour la sécurité numérique en Suisse ADSS détermine le moment où la liste de contrôle définitive est remise au prestataire de services informatiques. Il faut tenir compte du fait que la liste de contrôle est nécessaire pour la formation et l'atelier avec le fournisseur de services informatiques.

Après l'audit CyberSeal, le rapport d'audit est disponible en ligne pour les fournisseurs de services informatiques dans leur portail client sur digitalsecurityswitzerland.ch.

Les points critiques du BACS et des compagnies d'assurance doivent obligatoirement donner lieu à un audit de consortium.

4.2 Degré de conformité aux exigences de l'audit

Le label de qualité CyberSeal peut être attribué même si tous les clients du prestataire de services informatiques ne remplissent pas tous les aspects de la sécurité informatique. Cela peut être le cas, par exemple, lorsque le traitement des problèmes hérités du passé de la PME est coûteux ou prend beaucoup de temps, ou lorsque la correction des aspects de sécurité n'est pas souhaitée par la PME. Le prestataire de services informatiques devrait attirer l'attention de ces clients sur les aspects de sécurité incomplets au moins une fois par an, la correction pouvant prendre plusieurs années.

Dans ce cas, le degré de conformité du CyberSeal n'est pas de 100%. Le niveau de conformité minimal requis pour obtenir le label de qualité CyberSeal est déterminé par l'auditeur. Il est essentiel que le niveau de conformité s'améliore de manière visible chaque année.

4.3 Déclaration par le prestataire de services informatiques

Au moins 10 jours avant l'audit, le prestataire de services informatiques doit fournir à l'auditeur une déclaration de la liste de contrôle complète du CyberSeal. Pour la "distinction dans le type d'audit" (Voir chapitre 4.5), les questions déclarées avec auto-déclaration (S) dans la liste de contrôle ne sont abordées qu'en cas d'ambiguïté. Il est important de répondre au mieux à toutes les questions avant l'audit (y compris les questions désignées par I (interview) ou K (audit de console) dans la liste de contrôle).

4.4 Priorisation des exigences d'audit

Les exigences en matière d'audit sont classées par ordre de priorité comme suit :

- Priorité 1 : il s'agit d'exigences minimales qui doivent impérativement être mises en œuvre. Une implémentation partielle entraîne un écart mineur qui doit impérativement être traité avant le prochain audit. Le traitement doit entraîner une amélioration significative du respect des exigences (voir chapitre 4.2 "Degré de réalisation des exigences d'audit").
- Priorité 2 : ces exigences devraient être remplies par les bons fournisseurs de services informatiques (meilleures pratiques). Un non-respect n'entraîne pas d'écart mineur. L'auditeur peut toutefois formuler une remarque.
- Priorité 3 : cette exigence est considérée comme raisonnable par les spécialistes de la sécurité informatique. Dans l'environnement des PME, cette exigence n'est actuellement pas considérée comme absolument nécessaire.

4.5 Distinction dans le type d'examen

Les chapitres des exigences d'audit sont examinés différemment :

- **Auto-déclaration** : en règle générale, les chapitres ne sont pas discutés lors de l'audit. Il s'agit avant tout de chapitres dont le non-respect n'entraîne généralement pas de dommages importants dans l'environnement des PME. Il appartient au prestataire de services informatiques de mettre en œuvre les détails mentionnés dans la liste de contrôle. L'auditeur peut toutefois discuter et clarifier certaines questions de ces chapitres si les réponses du prestataire informatique ne sont pas comprises par lui.
- **Interview** : Ces chapitres sont également des questions importantes pour les PME en matière de cybersécurité. L'auto-déclaration remplie sera vérifiée lors de l'audit par le biais d'interviews.
- **Audit de console** : il s'agit de chapitres jugés très critiques pour les dommages dans l'environnement des PME. Lors de l'audit de consortium, l'auditeur effectue un contrôle concret de la mise en œuvre.

4.6 Exclusion de certains chapitres

Si certains chapitres de la liste de contrôle n'ont pas de sens pour un prestataire de services (p. ex. le prestataire de services n'exploite pas sa propre infrastructure de messagerie et ne le propose pas non plus à ses clients), l'auditeur peut exclure ces chapitres du contrôle. L'auditeur désigne alors ce chapitre par "Non disponible" (ND) dans le champ "Résultat".

4.7 Divergences

L'auditeur utilise la colonne "Résultat" pour évaluer la réalisation / la non-réalisation des différentes questions. Pour ce faire, il utilise exclusivement les abréviations suivantes :

- **OK :** l'exigence est suffisamment remplie

En ce qui concerne les écarts, une distinction est faite entre

- **DMA (divergences majeures)** : Elles empêchent l'attribution du label de qualité. Un point du référentiel n'a pas été respecté. Les écarts principaux sont toujours formulés par l'auditeur. Pour un chapitre intitulé "Autodéclaration", il n'y a pas d'écarts principaux.

S'il existe un ou plusieurs écarts majeurs, le client dispose de trois mois pour y remédier. A l'issue de ce délai, l'auditeur évalue la correction de l'écart principal.

- **DMI (divergences mineures)**: Elles n'empêchent pas l'attribution du label de qualité. Un point du référentiel n'a été que partiellement mis en œuvre. L'écart secondaire doit être traité jusqu'au prochain maintien et sera examiné en détail lors du prochain audit. Une réalisation non à 100% de l'écart secondaire peut à nouveau être déclarée comme écart secondaire lors du prochain audit. Il doit cependant y avoir eu une amélioration reconnaissable.

- **RE (Remarques)** : Les remarques sont des constatations de l'auditeur qui peuvent conduire à une amélioration. Elles doivent être examinées. Le prestataire de services informatiques décide si et comment les remarques doivent être mises en œuvre.

4.8 Déroulement pour l'obtention du label de qualité

Le déroulement chronologique est le suivant :

- Déclaration du prestataire de services informatiques.
- Audit pour l'obtention du label de qualité, nouvel audit tous les 3 ans selon les normes actuelles.
- Audit de maintien, chaque année entre les audits.

4.8.1 Préparation

L'Alliance pour la sécurité numérique en Suisse ADSS propose des ateliers d'orientation. Lors de ces ateliers gratuits, la liste de contrôle est notamment expliquée. Il est recommandé d'assister à cet atelier. Si le prestataire de services informatiques ne voit aucun problème pour l'obtention du label de qualité (c'est-à-dire que pour tous les points, au moins toutes les exigences de priorité 1 sont suffisamment remplies), il peut s'inscrire à l'audit.

4.8.2 Déclaration

Le prestataire de services informatiques télécharge la liste de contrôle. Il remplit tous les points. La déclaration remplie fait partie intégrante de l'inscription. La déclaration doit être envoyée au moins 10 jours avant l'audit.

4.8.3 Audit

Lors de l'audit, l'auditeur vérifie que les exigences d'audit avec la catégorie "entretien" sont correctes. Les exigences avec la catégorie "audit de console" doivent obligatoirement être vérifiées physiquement, c'est-à-dire que le prestataire de services informatiques doit montrer la mise en œuvre concrète. C'est à l'auditeur de décider comment vérifier une question particulière de la liste de contrôle. Il peut par exemple examiner la documentation et la configuration des outils correspondants. L'audit sur place dure quatre heures. Il faut consacrer au moins 1 heure à l'"interview" et 2 à 3 heures à l'"audit de console". L'auditeur consacre environ 4 heures à l'examen préalable de la déclaration et à l'intégration des remarques dans la liste de contrôle. Le label de qualité est attribué s'il n'y a pas d'écarts majeurs. Les éventuels écarts principaux doivent être discutés à la fin de l'audit. Le client doit savoir qu'il n'obtiendra pas le certificat.

4.8.4 Audit de maintien

Chaque année, en l'absence d'audit, un audit de maintien doit avoir lieu. L'audit de maintien est réalisé de manière autonome par le prestataire de services informatiques. Le prestataire de services informatiques décrit tous les travaux effectués, les écarts secondaires et les remarques. Cette description du prestataire de services informatiques est examinée par un auditeur et discutée avec le prestataire de services informatiques dans le cadre d'une session à distance. La session à distance dure environ une heure et peut prendre la forme d'un entretien téléphonique ou d'une vidéoconférence.

4.9 Coûts des audits

Les coûts de l'audit correspondent aux prix actuels déposés sur www.digitalsecurityswitzerland.ch.

4.10 Exigences envers l'auditeur

L'auditeur doit être un expert reconnu en matière de sécurité de l'information. Il doit connaître l'évolution actuelle et pouvoir expliquer une mise en œuvre correcte. Il doit également être en mesure d'évaluer techniquement des mises en œuvre inhabituelles. Les formations continues de l'expert technique doivent être attestées.

L'orientation client et l'amabilité de l'auditeur sont importantes.

- La formation des auditeurs a lieu dans les locaux de l'Alliance pour la sécurité numérique en Suisse ADSS à Zoug. La formation doit assurer les objectifs suivants :
- Les auditeurs connaissent en détail les documents importants du standard CyberSeal. Il s'agit du manuel d'audit CyberSeal, de la liste de contrôle CyberSeal et du modèle de rapport d'audit CyberSeal.
- Les auditeurs connaissent les principaux processus de l'administration.
- Les auditeurs connaissent les outils utilisés (site web), les conditions requises pour l'ordinateur utilisé (ordinateur portable) et les possibilités de transfert sécurisé des données.
- Les auditeurs procèdent à des audits aussi uniformes que possible.

La formation proprement dite des auditeurs est complétée par une formation continue annuelle. Pendant cette formation continue, les modifications du standard sont discutées et un échange d'expériences a lieu entre les auditeurs. Cet événement peut également avoir une influence sur le standard.

Alliance Sécurité Numérique Suisse ADSS est responsable de la nomination des auditeurs. Les conditions sont fixées par l'ADSS. En règle générale, il est souhaitable que les auditeurs suivent une formation. L'ADSS établit également un document qui réglemente la formation des auditeurs et définit les coûts de la formation.

4.11 Réalisation de l'audit

Dans la mesure du possible, l'audit est effectué physiquement sur place. Cela augmente la probabilité de découvrir des points critiques. Dans des cas particuliers (temps de déplacement, pandémie, etc.), les audits peuvent également être réalisés à distance. L'auditeur décide, en concertation avec Alliance Sécurité Numérique Suisse ADSS, si un audit peut être réalisé à distance.

4.12 Organisme responsable du label de qualité

L'organisme responsable du label de qualité est l'Alliance pour la sécurité numérique en Suisse ADSS. ADSS gère une succursale (actuellement à Zoug) avec une administration correspondante. L'administration a entre autres les tâches suivantes :

- Responsable du développement de la norme. L'ADSS peut déléguer le développement à un groupe de travail. Actuellement, il existe un groupe de travail appelé "Audit Committee", qui est responsable du développement de la norme.
- Responsable du site web avec les fonctions correspondantes pour une inscription automatisée des prestataires de services informatiques.
- Garantir un transfert de données sécurisé entre ADSS, les auditeurs et les clients.
- S'assurer que les audits sont effectués (y compris le maintien et un nouvel audit CyberSeal après trois ans) et qu'il y a une communication suffisante entre les fournisseurs de services informatiques et les auditeurs.
- Tenir à jour la liste des auditeurs actuels.
- Coordination et interlocuteur en cas de réclamation et d'avis divergents entre les auditeurs, les clients et ADSS.
- Délivrer le label de qualité.
- Marketing et finances.

4.13 Procédure en cas d'avis divergents

Si un prestataire de services informatiques conteste le résultat de l'audit, le cas est évalué par un deuxième auditeur et une décision finale est prise. La coordination du deuxième avis est prise en charge par l'administration.

Le délai de réclamation est de 30 jours à compter de la réception du rapport d'audit.

4.14 Manuel de sécurité pour la pratique

Il existe le "Manuel de sécurité pour la pratique" de l'entreprise isec ag. Le manuel de sécurité a été rédigé indépendamment de la norme, mais il décrit les mises en œuvre possibles pour atteindre la norme. Le manuel peut être considéré comme une boîte à outils. Les détails peuvent être consultés sur le site Internet suivant : https://sihb.ch.

5 Exigences en matière d'audit

L'audit CyberSeal est réalisé par l'auditeur sur la base de la liste de contrôle CyberSeal.

Les différentes questions de la liste de contrôle CyberSeal sont classées par ordre de priorité comme décrit au chapitre 4.4. En outre, la liste de contrôle CyberSeal définit, conformément au chapitre 4.5, quelles sections doivent être réalisées par auto-déclaration, par entretien ou par audit de console. L'utilisation de la liste de contrôle CyberSeal garantit une exécution uniforme des audits CyberSeal et définit la norme CyberSeal actuelle.

Les principaux éléments de la liste de contrôle du CyberSeal sont décrits ci-dessous. La formulation obligatoire de chaque point d'audit peut être consultée dans la liste d'audit.

5.1 Répartition des tâches client/prestataire informatique

La répartition des tâches entre le prestataire de services informatiques et la PME doit être décrite par écrit et de manière suffisamment détaillée. La documentation doit

- décrire les tâches du prestataire de services informatiques,
- définir les tâches que le client doit effectuer lui-même.
- Décrire les responsabilités du prestataire de services informatiques et celles de la PME

Il doit aussi être clair, en particulier, qui est responsable de quels aspects de la sécurité.

Il n'est pas nécessaire d'établir un document spécifique pour chaque client. Des contrats de maintenance ou une description de service peuvent suffire.

5.2 Gestion de l'accès à l'infrastructure du client

Le prestataire de services informatiques doit montrer comment il réglemente et gère les accès à l'infrastructure du client.

Les objectifs suivants doivent être atteints :

- Il faut s'assurer que le client puisse changer de prestataire de services informatiques à tout moment.
- Une sécurité élevée est mise en place pour l'accès à l'infrastructure du client (authentification multiple). Les collaborateurs qui quittent un prestataire de services informatiques n'ont en aucun cas accès à l'infrastructure du client.
- Le client doit être conscient des informations auxquelles le prestataire de services informatiques peut avoir accès.

5.3 Crédentiels et autorisations

Par "credentials", on entend normalement le nom d'utilisateur et le mot de passe. Il faut s'assurer que les points suivants sont remplis :

- Il faut mettre en place un processus qui permette de retracer chaque modification de credentials (y compris la réinitialisation de mots de passe) et d'autorisations. Le processus doit également inclure les autorisations temporaires.
- En cas d'urgence, le client peut accéder à tous ses credentials et autorisations.
- Les mots de passe du client sont conservés en toute sécurité (par ex. coffre-fort pour mots de passe).

5.4 Documentation

Le prestataire de services informatiques doit posséder une documentation à jour sur l'infrastructure de la PME. Cette documentation comprend au minimum

- Tous les systèmes sont répertoriés sur une vue d'ensemble.
- La documentation des systèmes peut être remise au client. Aucun système spécial n'est nécessaire pour lire la documentation.
- Le prestataire de services informatiques met régulièrement à jour la documentation.

5.5 Conception du réseau

La conception du réseau tient compte des différentes zones ;

- Zone bureau
- Zone de fabrication, des dispositifs non patchables peuvent parfois se trouver dans cette zone.
- Zone publique pour les invités et les appareils privés des collaborateurs.

Il faut veiller à ce que les transitions entre les zones n'autorisent que le trafic minimal nécessaire. Il faut en tout cas utiliser des routeurs ou des appareils similaires qui supportent les règles correspondantes.

5.6 Pare-feu

Les conditions-cadres suivantes doivent être remplies :

- Les différentes connexions du pare-feu n'autorisent que le trafic nécessaire. Le trafic sortant vers Internet doit également être limité.
- Les règles de pare-feu doivent être lisibles par un spécialiste externe.
- Le Ruleset doit être régulièrement contrôlé. Une vérification doit être compréhensible.

5.7 WLAN

Le WLAN chez le prestataire de services informatiques et dans la PME s'oriente en principe sur le concept présenté au chapitre 5.5. Les exigences suivantes sont en outre définies :

- Des mots de passe distincts et non déductibles doivent être utilisés pour chaque client.
- Un réseau WLAN séparé doit être mis en place pour les appareils privés des collaborateurs et pour les invités.
- L'authentification au moyen de credentials partagés ne peut être utilisée que pour les zones de réseau publiques. L'accès à toutes les autres zones (selon le chapitre 5.5) doit se faire exclusivement avec des identifiants personnels.
- Seuls des mécanismes de protection actuels et sûrs sont utilisés.

5.8 Gestion des identités (Active Directory, Azure, etc.)

Il est garanti que les éléments suivants sont mis en œuvre :

- Le client peut administrer lui-même l'AD ou peut confier cette tâche à un autre prestataire de services. Cela peut être garanti en confiant au client un compte d'administrateur de secours.
- Les comptes avec des autorisations étendues ne sont pas utilisés pour le travail quotidien des applications.
- Les portails accessibles au public et les infrastructures en nuage auxquelles il est possible d'accéder au moyen de credentials AD sont mis en œuvre de manière sécurisée.
- Seuls des comptes d'administrateur personnalisés sont utilisés.

5.9 Hardening des composants informatiques

Tous les systèmes et appareils des clients configurés par le prestataire de services informatiques sont renforcés. Il existe typiquement une liste de contrôle, avec les paramètres nécessaires.

5.10 Système de messagerie

Selon les données du BACS et des assurances, une cyberattaque commence par une prise de contact par e-mail. Ce point revêt donc une importance particulière.

Si l'infrastructure de messagerie est exploitée localement, les exigences minimales suivantes s'appliquent :

- L'infrastructure de messagerie doit être mise en place et exploitée de manière sûre. Une protection contre les logiciels malveillants est nécessaire ainsi que le contrôle de l'authenticité de l'expéditeur, ce qui peut être réalisé par l'installation de SPF ou de DKIM. L'accès avec des appareils mobiles est contrôlé et limité en conséquence.

Dans de nombreux cas, l'infrastructure de messagerie des clients est exploitée dans le cloud. Chez la plupart des fournisseurs, cela permet de garantir une sécurité très élevée.

5.11 Gestion des correctifs

Un patching insuffisant et rapide est considéré par le BACS et les assurances comme la cause de nombreuses attaques dans le cyberenvironnement. En outre, selon les vulnérabilités existantes, celles-ci peuvent être utilisées pour étendre les autorisations. Ce point revêt donc une importance particulière.

Au minimum, les exigences suivantes doivent être mises en œuvre :

- La gestion des correctifs est définie dans un processus qui doit impérativement être respecté. Le processus comprend également la gestion des correctifs des produits non Microsoft. Les cycles de patch sont choisis de manière judicieuse.
- Les exceptions à la gestion des correctifs (par exemple, Java pour une application ne doit pas être corrigé) doivent être consignées par écrit.
- En cas de vulnérabilités majeures et graves (par ex. vulnérabilité Exchange), un processus d'urgence doit impérativement être lancé.

5.12 Appareils mobiles

Actuellement, les appareils mobiles ne sont pas la cause d'incidents majeurs de cybersécurité dans les PME. Néanmoins, une sécurité minimale doit être garantie.

- Les supports de données sur les appareils mobiles doivent être cryptés dans la mesure du possible.
- L'accès aux données de l'entreprise n'est possible qu'après une authentification suffisante.

De nombreux paramètres peuvent être imposés techniquement par des politiques. L'utilisation de politiques peut être utile et efficace pour les PME.

5.13 Travail à distance / bureau à domicile

De nombreux prestataires de services informatiques sont en mesure de répondre aux exigences des clients, même si les employés du prestataire de services informatiques travaillent à domicile. De plus, le travail à domicile permet également de garantir les services promis en cas de pandémie.

C'est pourquoi les environnements de bureau à domicile sécurisés sont d'une grande importance :

- Le prestataire de services informatiques élabore et met en œuvre un concept de travail à distance judicieux et sûr.
- Le concept garantit qu'aucune connexion réseau directe ne peut être établie entre les systèmes du client et le bureau à domicile.
- Il convient de mettre en œuvre une forme d'authentification multiple.
- Le concept décrit également les fonctions supplémentaires autorisées (par ex. impression, mappage de lecteur, etc.).

5.14 Protection contre les logiciels malveillants

Une bonne protection contre les malwares (virus) permet d'éviter de nombreuses infections. Le BACS et les assurances accordent une grande importance à une bonne protection contre les logiciels malveillants. Des tests ont montré par le passé qu'il existe de grandes différences entre les nombreux produits disponibles sur le marché. Le choix du produit concrètement utilisé devient donc très important.

La plupart des serveurs et des clients sont en général assez bien protégés. De nombreuses attaques ont lieu via un système de messagerie. Il est donc impératif d'adopter une approche à deux niveaux (pare-feu et client) pour les systèmes de messagerie.

Il est courant, y compris dans les PME, que l'accès à Internet soit particulièrement protégé.

Il est encore courant de ne pas pouvoir installer de protection contre les logiciels malveillants sur certains systèmes. La raison doit en être documentée. En outre, de tels systèmes doivent être isolés du point de vue du réseau.

5.15 Sauvegarde / Restauration

Le BACS et les assurances définissent une bonne sauvegarde comme essentielle pour la survie d'une entreprise en cas de cyberattaque. Lors d'une cyber-attaque, on essaie souvent de rendre la sauvegarde inutilisable.

Une bonne sauvegarde joue donc un rôle très important. Outre une bonne documentation de la sauvegarde, son fonctionnement doit être testé fréquemment. Il ne s'agit pas seulement de restaurer des fichiers individuels, mais aussi de restaurer complètement des systèmes entiers et de vérifier leur fonctionnalité. Les environnements de virtualisation et les outils de sauvegarde actuels prennent en charge un tel test régulier.

Même les grandes entreprises attachent de l'importance à ce que la sauvegarde ne puisse plus être

modifiée ultérieurement. La bande comme support de sauvegarde connaît donc actuellement un "come back". De nombreux projets utilisent également des supports de données amovibles. Ceux-ci sont moins sûrs que les bandes, mais souvent moins chers.

Une copie de la sauvegarde doit être conservée séparément sur le plan local.

5.16 Gestion du changement/gestion des incidents

L'accent de ce thème est mis sur la traçabilité. Cela peut également être important en cas de cyber-attaque. Le prestataire de services informatiques veille à ce que toutes les modifications apportées au système puissent être retracées. De même, tous les incidents (Incidents) peuvent être retracés.

Chez les prestataires de services informatiques des PME, cette gestion est parfois négligée. Mais ils ne tiennent pas compte du fait que beaucoup de temps peut être économisé si un incident (Incident) ou un changement peut être facilement trouvé. De plus, les systèmes supportent d'eux-mêmes une gestion primitive des changements. Il faut toutefois utiliser ces systèmes de manière conséquente.

5.17 Consignation des données

Chaque système supporte une assez bonne journalisation. Il peut toutefois être nécessaire d'activer ou de configurer cette journalisation. On peut le faire à l'aide d'une liste de contrôle (voir aussi le chapitre 5.9). C'est un point important d'un SLA. La durée de conservation et les valeurs à consigner devraient y être définies.

5.18 Suivi

Un bon monitoring peut être très efficace pour un prestataire de services informatiques. Le système de monitoring peut soutenir ou mettre en œuvre la gestion des changements. En outre, un monitoring peut détecter de nombreuses attaques.

Une surveillance proactive peut continuer à détecter les cyber-attaques et à aider à l'évaluation des dommages.

L'étendue du monitoring doit être définie dans le cadre de SLA avec les clients. Les constatations doivent faire l'objet de rapports réguliers au client.

5.19 Élimination des supports de données & Effacement des données

Des informations sensibles sont stockées sur chaque support de données. Le prestataire de services informatiques doit garantir que ces données ne tombent pas entre des mains étrangères. En général, le support de données est détruit physiquement.
Le prestataire de services informatiques attire l'attention du client sur l'obligation de supprimer régulièrement les données sur ses systèmes.

5.20 Services de tiers

Aujourd'hui, chaque prestataire de services informatiques doit installer des produits de tiers chez les clients. Le client peut par exemple décider de travailler avec Office 365 ou de faire appel à certains services cloud. Le prestataire de services informatiques connaît ces produits et peut configurer un niveau de sécurité comparable à celui des services locaux.

5.21 Gestion des menaces et des vulnérabilités chez les clients

De nombreux clients utilisent du matériel ou des logiciels obsolètes et peu sûrs. Le prestataire de services informatiques attire l'attention du client sur ce point. Il est préférable de le faire lors d'un entretien régulier. Il est vivement recommandé de rédiger une brève note de conversation reprenant les décisions

essentielles.

5.22 Formation du personnel

Ce point est considéré comme très critique par BACS et les assurances. Une grande partie des cyber-attaques commencent par un e-mail compromis. Chaque collaborateur doit impérativement être en mesure de reconnaître les faux e-mails et d'adopter le bon comportement. C'est pourquoi les clients et les prestataires de services informatiques doivent être formés régulièrement. Cette formation comprend également le comportement correct du collaborateur lors de la réception de ces faux e-mails.

5.23 Concept d'urgence

La BACS et les assurances considèrent que l'élaboration d'un plan d'urgence est très importante.

Un concept d'urgence garantit que l'on pense à tout lors d'un événement extraordinaire et que les préparatifs nécessaires peuvent être élaborés et testés sans précipitation. Le concept d'urgence doit couvrir les événements les plus importants. Actuellement, la cybercriminalité (ransomware,

cryptage des données, vol de données et menace de publication), qui doit impérativement être couverte.

Une urgence peut survenir aussi bien chez le prestataire de services informatiques que chez les clients d'un prestataire de services informatiques. Il est donc judicieux d'élaborer un concept d'urgence compatible au moins dans l'environnement informatique. Il sera nécessaire d'inclure le prestataire de services informatiques dans le concept d'urgence d'un client final.

Dans l'environnement informatique, le concept d'urgence doit définir qui assure la communication avec l'extérieur et comment. Il définit en outre les services qui doivent être informés pour remédier à l'urgence (police, BACS, assurances, entreprises de soutien, etc.) Les adresses de contact correspondantes font partie intégrante du concept d'urgence.

Dans l'environnement informatique, le traitement des données cryptées doit être réglementé. Il faut s'assurer qu'une récupération des données est possible, par exemple, même en cas de panne d'un AD. Il est important de tester régulièrement le concept d'urgence. Ils permettent de former les personnes clés et de détecter les points faibles.

5.24 Dates d'expiration

Il y a de plus en plus de composants informatiques qui cessent de fonctionner après une date d'expiration (licences, certificats, processus de maintenance des composants, etc.) Tous les composants qui ont une date d'expiration doivent être surveillés par le prestataire de services informatiques.

L'obsolescence du matériel constitue un autre risque. Si les patchs de sécurité ne sont plus disponibles, les composants doivent être remplacés.

5.25 Sécurité physique

La sécurité physique doit être assurée par le prestataire de services informatiques. L'accès aux locaux du prestataire de services informatiques doit être réglementé. En particulier, l'accès aux éventuels centres de données du prestataire de services informatiques doit être limité au minimum.

Les appareils du prestataire de services informatiques doivent être protégés de manière judicieuse contre les influences extérieures (onduleur, refroidissement, connexion Internet redondante, etc.)

5.26 Gestion des risques

Un prestataire de services informatiques doit pratiquer une gestion des risques judicieuse. Les principaux risques doivent être connus. Les risques peuvent être atténués par les mesures suivantes :

- Prévention des risques : dans certaines circonstances, une évaluation des risques peut conduire à l'impossibilité de proposer certains services.
- Réduction des risques : des mesures sont prises pour réduire un risque donné. Tous les chapitres précédents du chapitre 5 sont des mesures de réduction des risques.
- Transfert de risques : certains risques peuvent être assurés. Le type d'assurance (responsabilité civile professionnelle, cyber-dommages, dommages financiers, etc.), la somme assurée et les prestations supplémentaires (par exemple, assistance en cas de cyber-attaque) doivent être choisis avec soin.
- Acceptation des risques : chaque entreprise doit assumer certains risques (ou risques résiduels). Le fait de porter des risques doit impérativement être accepté par la direction de l'entreprise du prestataire de services informatiques et ne peut pas être délégué.

Un prestataire de services informatiques devrait aider ses clients à mettre en place leur propre gestion des risques. Un prestataire de services informatiques peut les aider dans de nombreux cas et répondre à leurs questions.

Comité d'auditeurs de l'Alliance pour la sécurité numérique en Suisse

6 Annexe

Liste des abréviations

ADSS	Alliance pour la sécurité numérique en Suisse ADSS
BACS	Office fédéral de la cybersécurité
BSI	Office fédéral de la sécurité des technologies de l'information
Cobit	Objectifs de contrôle pour l'information et les technologies connexes
DKIM	DomainKeys Identified Mail
CEI	Commission électrotechnique internationale
TIC	Technologies de l'information et de la communication
ISO	Organisation internationale de normalisation
PME	Petite(s) et moyenne(s) entreprise(s) [Petite(s) et Moyenne(s) Entreprise(s)
NCSC	Centre national de cybersécurité
NIST	Institut national des normes et de la technologie
SLA	Service Level Agreement (accord sur le niveau de service)
SPF	Cadre de la politique d'envoi

Abréviations Liste de contrôle

DMA	Divergence majeure
DMI	Divergence mineure
ND	Non disponible
RE	Remarque
IC	Infrastructure du client
PI	Propre infrastructure
A	Auto-déclaration
E	Entretien
T	Terminaux (Console)