CyberSeal Manuel d'audit

Version 3.0, 08 mars 2026

Table des matières

1 Objet du document 4
2 Le label de qualité CyberSeal 4
3 Bases 5
3.1 Définitions 5
3.2 Périmètre du label 5
3.3 Distinction par rapport à d'autres certifications/référentiels 5
4 Aspects organisationnels de l'audit 7
4.1 Standard CyberSeal 7
4.2 Niveau de conformité aux exigences d'audit 7
4.3 Déclaration par le prestataire informatique 7
4.4 Hiérarchisation des exigences d'audit 7
4.5 Distinction selon le mode de vérification 8
4.6 Exclusion de certains chapitres 8
4.7 Écarts 8
4.8 Processus d'obtention du label 9
4.9 Coûts des audits 9
4.10 Exigences envers l'auditeur 9
4.11 Réalisation de l'audit 10
4.12 Organisme responsable du label 10
4.13 Procédure en cas de désaccord 10
4.14 Guide de sécurité pratique 11
5 Exigences d'audit 11
5.1 Répartition des tâches client/prestataire informatique 11
5.2 Gestion des accès à l'infrastructure client 11
5.3 Identifiants et droits d'accès 11
5.4 Documentation 12
5.5 Architecture réseau 12
5.6 Pare-feu 12
5.7 WLAN 12
5.8 Gestion des identités (Active Directory, Azure, etc.) 13
5.9 Durcissement des composants informatiques 13
5.10 Messagerie électronique 13
5.11 Gestion des correctifs 13
5.12 Appareils mobiles 13
5.13 Télétravail / Bureau à domicile 14
5.14 Protection contre les logiciels malveillants 14

5.15 sauvegarde / restauration 14
5.16 Gestion des changements / Gestion des incidents 15
5.17 Journalisation 15
5.18 Monitoring/gestion des vulnérabilités 15
5.19 Élimination des supports de données / Suppression des données 15
5.20 Services de tiers 15
5.21 Gestion de l'intelligence artificielle 15
5.22 Formation du personnel 16
5.23 Plan d'urgence 16
5.24 Échéances à surveiller 16
5.25 Sécurité physique 17
5.26 Gestion des risques 17
5.27 Protection des données et aspects juridiques 17
5.28 Développement logiciel 18
6 Annexe 19

1 Objet du document

Ce manuel décrit en détail l'application de la liste de contrôle CyberSeal. Il décrit également le processus d'audit, les coûts, le cadre général et d'autres détails relatifs à l'attribution du label CyberSeal. Le manuel est révisé annuellement.

2 Le label de qualité CyberSeal

Lorsque l'audit est réussi, l'Alliance pour la Sécurité Numérique Suisse (ADSS) décerne au prestataire informatique le label CyberSeal. Ce label atteste que le prestataire a passé l'audit sans écart majeur.

Le label est valable 3 ans, à condition que les audits de maintien des années deux et trois aient été réussis.

Das label Le label CyberSeal repose sur le constat que la grande majorité des PME collabore étroitement avec un prestataire informatique principal, car une PME n'est généralement pas en mesure de garantir seule les aspects d'une infrastructure informatique sûre et conforme aux standards actuels. Le niveau de sécurité atteint par une PME dépend donc en grande partie de son prestataire informatique principal. Le label définit les mesures de sécurité que le prestataire informatique doit mettre en œuvre pour lui-même et ses clients. La PME peut avoir confiance qu'un prestataire informatique labellisé CyberSeal prend suffisamment en compte les aspects essentiels de la cybersécurité.

Lors de l'audit CyberSeal, le questionnaire de la liste de contrôle CyberSeal est complété. Les questions sont classées par ordre de pertinence. Cette classification a été conçue pour que le label reste accessible aux prestataires informatiques de taille modeste.

Les aspects de sécurité prioritairement pris en compte sont ceux qui sont essentiels pour les PME et fréquemment exploités par des attaquants potentiels dans ce contexte. Pour le développement du standard, les signalements des assureurs et des organisations étatiques comme le BACS (NCSC, Melani) concernant les dommages réellement survenus au cours de l'année écoulée sont très importants. L'objectif est de remédier aux vulnérabilités les plus connues et fréquemment exploitées au sein des PME.

Le label CyberSeal exige un haut niveau d'actualité. Les dernières évolutions en matière de menaces et de types de dommages sont intégrées annuellement dans le standard mis à jour.

Le label CyberSeal se distingue des labels, certifications et référentiels courants en sécurité de l'information (tels qu'ISO/IEC 27001) sur plusieurs points :

- Le label tient compte de l'intégration de l'informatique dans les PME suisses. Il s'adresse en particulier aux PME et à leurs prestataires informatiques.
- Le label garantit que le prestataire informatique met en œuvre les mesures de sécurité les plus pertinentes pour les PME courantes. L'accent est mis sur la cybersécurité.
- Le label est nettement plus facile à obtenir qu'une certification ISO/IEC 27001.
- Le label permet aux PME d'identifier un prestataire informatique de qualité.
- Le label reflète le paysage des menaces actuelles.

3 Bases

3.1 Définitions

prestataire informatique: Le prestataire informatique est une entreprise qui fournit des services informatiques à diverses PME. Il constitue ainsi le point de confiance central en matière de sécurité informatique pour les PME. On recense environ 5'000 entreprises en Suisse considérées comme prestataires informatiques.

PME: Une PME est une petite ou moyenne entreprise. Dans le cadre du label, on part du principe qu'une PME est plutôt de petite taille et s'appuie sur les recommandations d'un prestataire informatique pour les questions de sécurité informatique.

Drittanbieter: Prestataires supplémentaires mandatés par le prestataire informatique ou la PME pour fournir des services. Le prestataire informatique est responsable de l'intégration sécurisée de ces fournisseurs tiers. Les fournisseurs tiers peuvent être très variés : éditeurs d'applications (ex. Abacus), Dropbox, Office 365 et autres fournisseurs cloud.

auditeur: Un auditeur désigné par l'organisation responsable Allianz Digitale Sicherheit Schweiz ADSS, habilité à décerner le label. L'ADSS peut déléguer la nomination des auditeurs à d'autres entreprises du secteur de l'audit (ex. BDO, etc.).

Compte privilégié: compte disposant de droits élevés en matière de système, de configuration et/ou d'écriture.

authentification multifacteur: En général, deux facteurs distincts sont utilisés pour l'authentification. Dans ce document, cela inclut les méthodes courantes basées sur un jeton (SMS, Authenticator, etc.) ainsi que des méthodes complémentaires telles que les plages d'adresses IP restreintes et les équipements protégés par certificat.
Les authentifications multiples successives (ex. connexion système suivie d'une connexion applicative) ne sont pas considérées comme de l'authentification multifacteur.

Mots de passe forts : Le BACS décrit sur le site web Protégez vos comptes / mots de passe (admin.ch) les conditions permettant de considérer des mots de passe comme une authentification suffisamment sécurisée.

Documentation: Une documentation désigne toute forme d'information qui est accessible, traçable, périodiquement vérifiée et soumise à un processus de gestion des modifications. Une documentation peut notamment être présente dans le code source ou une configuration.

Appareils mobiles : Appareils qui ne sont pas liés à un emplacement géographique fixe et/ou qui disposent d'une alimentation mobile (batterie intégrée). Les appareils mobiles typiques sont les laptops et les smartphones.

3.2 Périmètre du label

Le label est décerné aux prestataires informatiques qui construisent et exploitent l'infrastructure IT d'une PME. Pour les prestataires informatiques de grande taille, seule une partie de l'entreprise peut éventuellement être labellisée. Le périmètre doit être défini par le prestataire informatique. Si le périmètre ne couvre pas l'ensemble de l'entreprise et de ses services, le périmètre audité est mentionné sur le label.

3.3 Distinction par rapport à d'autres certifications/référentiels

Il existe d'autres certifications courantes et pertinentes en France. Remarque : CyberSeal parle délibérément de label et non de certification. Cela souligne que les exigences de CyberSeal sont moins élevées que celles d'une certification ISO/IEC 27001 par exemple.

3.3.1 ISO/IEC 27001

Il s'agit d'un standard international. En Suisse, la SAS (Service d'accréditation suisse), une division de la Confédération, est chargée de la mise en œuvre du standard. La SAS détermine quelles entreprises sont autorisées à réaliser des audits. Les organismes accrédités sont répertoriés sur le site web «Recherche d'organismes accrédités SAS (admin.ch)» . Il est courant qu'un organisme accrédité dans un pays réalise également des certifications à l'étranger.

L'accent est mis sur les grandes entreprises, notamment pour des raisons de coût, car une certification peut s'avérer relativement onéreuse.

Le standard est conçu de manière générique, ce qui permet de le maintenir relativement stable dans le temps. Actuellement, les audits sont réalisés selon la version de 2022.

Les développements récents (ex. protection des données, cloud computing) sont définis dans des standards complémentaires. Une certification selon ces standards complémentaires n'est pas possible. Ils indiquent néanmoins comment le standard principal doit être interprété.

3.3.2 BSI IT-Grundschutz

Le BSI IT-Grundschutz est élaboré et maintenu par le BSI allemand (Office fédéral de la sécurité de l'information). Il repose sur plus de 100 modules IT-Grundschutz (ex. APP 1.2 = Navigateur web, NET.3.2 = Pare-feu). Ces modules sont très orientés vers la pratique et décrivent par exemple une configuration sécurisée d'un composant. Il est toutefois difficile de maintenir ces modules suffisamment à jour.

En France, le BSI IT-Grundschutz joue un rôle important principalement dans l'administration publique. De nombreuses grandes entreprises prennent également en compte ce standard, au moins partiellement.

Il est à noter qu'il existe depuis quelque temps un standard BSI proprement dit, lequel est largement compatible avec les normes ISO.

3.3.3 Standard minimal TIC

Le standard minimal TIC est une norme suisse visant à améliorer la résilience des TIC. TIC désigne les Technologies de l'Information et de la Communication.

Ce standard a été publié par l'Office fédéral pour l'approvisionnement économique du pays et s'adresse en particulier aux exploitants d'infrastructures critiques.

Le standard minimal TIC repose essentiellement sur le référentiel NIST.

3.3.4 Autres référentiels

Il existe de nombreux autres référentiels tels que COBIT, le cadre NIST, qui jouent un rôle secondaire en France.

4 Aspects organisationnels de l'audit

4.1 Standard CyberSeal

Le standard comprend le manuel CyberSeal, la liste de contrôle CyberSeal et le rapport d'audit.

Le manuel d'audit du standard CyberSeal est publié sur le site web digitalsecurityswitzerland.ch. Une version abrégée de la liste de contrôle y est également disponible.

L'Alliance pour la Sécurité Numérique Suisse (ADSS) détermine le moment auquel la liste de contrôle définitive est remise au prestataire informatique. Il convient de tenir compte du fait que la liste de contrôle est nécessaire pour la formation et l'atelier avec le prestataire informatique.

Le rapport d'audit est disponible pour les prestataires informatiques après l'audit CyberSeal, en ligne dans leur espace client sur digitalsecurityswitzerland.ch.

Les points critiques identifiés par le BACS et les compagnies d'assurance doivent obligatoirement faire l'objet d'un audit console.

4.2 Niveau de conformité aux exigences d'audit

Le label CyberSeal peut être décerné même si tous les clients du prestataire informatique ne satisfont pas à l'ensemble des exigences de sécurité informatique. Cela peut être le cas lorsque la remise à niveau des installations existantes est coûteuse ou chronophage pour la PME, ou lorsque la PME ne souhaite pas remédier à certains aspects de sécurité. Le prestataire informatique doit alerter ces clients au moins une fois par an sur les lacunes en matière de sécurité, sachant que leur résolution peut prendre plusieurs années.

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

4.3 Déclaration par le prestataire informatique

Au moins 10 jours avant l'audit, le prestataire informatique doit fournir à l'auditeur une déclaration complète de la liste de contrôle CyberSeal. Concernant la «Distinction selon le type de vérification» (voir chapitre 4.5), seules les questions classées en Autodéclaration (S) dans la liste de contrôle feront l'objet d'un échange en cas d'ambiguïté. Il est important que toutes les questions soient répondues au mieux avant l'audit, y compris celles marquées I (Entretien) ou K (Audit console).

4.4 Hiérarchisation des exigences d'audit

Les exigences d'audit sont hiérarchisées comme suit :

- Priorité 1 : Ce sont des exigences minimales qui doivent impérativement être mises en œuvre. Une mise en œuvre partielle entraîne un écart mineur, qui doit obligatoirement être traité avant le prochain audit. Le traitement doit apporter une amélioration substantielle du taux de conformité (voir chapitre 4.2 «Taux de conformité aux exigences d'audit»).
- Priorité 2 : Ces exigences devraient être satisfaites par tout prestataire informatique de qualité (bonne pratique). Le non-respect ne génère pas d'écart mineur. L'auditeur peut toutefois formuler une remarque.
- Priorité 3 : Cette exigence est considérée comme pertinente par les experts en sécurité IT. Dans le contexte des PME, elle n'est pas jugée indispensable à l'heure actuelle.

4.5 Distinction selon le mode de vérification

Les chapitres des exigences d'audit sont vérifiés selon différentes modalités :

- **autodéclaration**: Les chapitres ne sont généralement pas discutés lors de l'audit. Il s'agit principalement de chapitres dont le non-respect n'entraîne généralement pas de dommages importants dans le contexte des PME. Il appartient au prestataire informatique de mettre en œuvre les détails figurant dans la liste de contrôle. L'auditeur peut toutefois aborder certaines questions de ces chapitres si les réponses du prestataire informatique ne sont pas clairement comprises.
- **Interview**: Ces chapitres portent sur des questions de cybersécurité importantes également pour les PME. La déclaration complétée est vérifiée lors de l'audit par le biais d'entretiens.
- **audit console**: Ce sont les chapitres jugés très critiques en termes de risques de dommages dans le contexte des PME. L'auditeur procède lors de l'audit console à une vérification concrète de la mise en œuvre.

4.6 Exclusion de certains chapitres

Si certains chapitres de la liste de contrôle ne s'appliquent pas à un prestataire (ex. le prestataire n'exploite pas sa propre infrastructure de messagerie et ne propose pas ce service à ses clients), l'auditeur peut les exclure de l'audit. L'auditeur indique «Non Disponible» (ND) dans le champ «Résultat» pour ce chapitre.

4.7 Écarts

L'auditeur utilise la colonne «Résultat» pour évaluer la conformité ou la non-conformité de chaque question. À cet effet, il utilise exclusivement les abréviations suivantes :

- **OK:** L'exigence est suffisamment satisfaite

Parmi les écarts, on distingue :

- **HA (écart majeuren)**: Ces écarts empêchent l'attribution du label. Un point du standard n'a pas été respecté. Les écarts majeurs sont toujours formulés par l'auditeur. Pour un chapitre classé en «Autodéclaration», il n'y a pas d'écarts majeurs.

Lorsqu'un ou plusieurs écarts majeurs sont constatés, le client dispose de 3 mois pour y remédier. À l'expiration de ce délai, l'auditeur évalue la résolution de l'écart majeur.

- **NA (écart mineuren)**: Ces écarts n'empêchent pas l'attribution du label. Un point du standard n'a été que partiellement mis en œuvre. L'écart mineur doit être traité avant le prochain audit de maintien et sera examiné en détail lors du prochain audit. Une conformité inférieure à 100 % peut à nouveau être déclarée comme écart mineur lors du prochain audit, mais une amélioration perceptible doit avoir eu lieu.

- **HW (remarques)**: Les remarques sont des observations de l'auditeur susceptibles de conduire à une amélioration. Elles doivent être examinées. Le prestataire informatique décide s'il y donne suite et de quelle manière.

4.8 Processus d'obtention du label

Le calendrier est le suivant :

- Déclaration du prestataire informatique.
- Audit pour l'obtention du label, nouvel audit tous les 3 ans selon le standard en vigueur.
- Audit de maintien, jährlich zwischen den Audits.

4.8.1 Préparation

L'Allianz Digitale Sicherheit Schweiz ADSS propose des ateliers d'orientation. Ces ateliers gratuits expliquent notamment la liste de contrôle. Il est recommandé d'y participer. Si le prestataire informatique ne voit pas d'obstacle à l'obtention du label (c'est-à-dire si toutes les exigences de priorité 1 sont suffisamment satisfaites), il peut s'inscrire à l'audit.

4.8.2 Déclaration

Le prestataire informatique télécharge la liste de contrôle et renseigne tous les points. La déclaration complétée fait partie du dossier d'inscription. Elle doit être soumise au moins 10 jours avant l'audit.

4.8.3 Audit

Lors de l'audit, l'auditeur vérifie la conformité des exigences de la catégorie «Entretien». Les exigences de la catégorie «Audit console» doivent obligatoirement être vérifiées physiquement, c'est-à-dire que le prestataire informatique doit démontrer la mise en œuvre concrète. L'auditeur décide de la manière dont chaque question de la liste de contrôle est vérifiée. Il peut par exemple consulter la documentation et la configuration des outils correspondants. L'audit sur site dure 4 heures : au moins 1 heure doit être consacrée aux «Entretiens» et 2 à 3 heures à l'«Audit console». L'auditeur consacre environ 4 heures à la vérification préalable de la déclaration et à l'intégration des remarques dans la liste de contrôle. Le label est délivré en l'absence d'écarts majeurs. Les éventuels écarts majeurs doivent être discutés à la fin de l'audit. Le client doit être informé qu'il ne recevra pas le label.

4.8.4 Audit de maintien

Chaque année sans audit complet, un audit de maintien doit avoir lieu. Cet audit de maintien est réalisé de manière autonome par le prestataire informatique. Celui-ci décrit toutes les actions menées en lien avec les écarts mineurs et les remarques. Cette description est vérifiée par un auditeur et discutée avec le prestataire informatique lors d'une session à distance. La session à distance dure environ 1 heure et peut prendre la forme d'un appel téléphonique ou d'une visioconférence.

4.9 Coûts des audits

Les coûts de l'audit correspondent aux tarifs en vigueur, disponibles sur www.digitalsecurityswitzerland.ch publiés.

4.10 Exigences envers l'auditeur

L'auditeur doit être un expert reconnu en sécurité de l'information. Il doit maîtriser les évolutions actuelles du domaine et être en mesure d'expliquer une mise en œuvre correcte. Il doit pouvoir évaluer techniquement même des implémentations inhabituelles. Les formations continues de l'expert doivent être documentées.

L'orientation client et l'amabilité de l'auditeur sont des qualités essentielles.

- La formation des auditeurs a lieu dans les locaux de l'Alliance pour la Sécurité Numérique Suisse (ADSS) à Zoug. Cette formation vise à atteindre les objectifs suivants :
- Les auditeurs connaissent en détail les documents importants du standard CyberSeal : le manuel d'audit CyberSeal, la liste de contrôle CyberSeal et le modèle de rapport d'audit CyberSeal.
- Les auditeurs connaissent les principaux processus administratifs.
- Les auditeurs connaissent les outils utilisés (site web), les exigences relatives à l'équipement informatique (laptop) et les modalités de transfert sécurisé des données.
- Les auditeurs conduisent les audits de manière aussi homogène que possible.

La formation initiale des auditeurs est complétée par une formation continue annuelle. Lors de celle-ci, les modifications du standard sont présentées et un échange d'expériences entre auditeurs a lieu. Cette rencontre peut également influencer l'évolution du standard.

L'Alliance pour la Sécurité Numérique Suisse (ADSS) est responsable de la nomination des auditeurs. Les conditions sont fixées par l'ADSS. En règle générale, la participation à la formation des auditeurs est requise. L'ADSS élabore également un document régissant la formation des auditeurs et définissant les coûts de cette formation.

4.11 Réalisation de l'audit

L'audit est réalisé autant que possible en présentiel sur site. Cela augmente la probabilité de détecter des points critiques. Dans des cas exceptionnels (délais de déplacement, pandémie, etc.), les audits peuvent également être réalisés à distance. L'auditeur décide, en concertation avec l'Alliance pour la Sécurité Numérique Suisse (ADSS), si un audit peut être effectué à distance.

4.12 Organisme responsable du label

L'organisme responsable du label est l'Allianz Digitale Sicherheit Schweiz ADSS. L'ADSS dispose d'une agence (actuellement à Zoug) avec une administration correspondante. L'administration assume notamment les tâches suivantes :

- Responsable de l'évolution du standard. L'ADSS peut déléguer ce développement à un groupe de travail. Il existe actuellement un groupe de travail appelé «Audit Committee», responsable du développement du standard.
- Responsable du site web avec les fonctionnalités permettant l'inscription automatisée des prestataires informatiques.
- Garantir un transfert sécurisé des données entre l'ADSS, les auditeurs et les clients.
- S'assurer que les audits sont réalisés (y compris les audits de maintien et le nouvel audit CyberSeal après trois ans) et qu'une communication suffisante a lieu entre les prestataires informatiques et les auditeurs.
- Tenir à jour la liste des auditeurs actifs.
- Coordination et interlocuteur en cas de réclamation et de désaccord entre auditeurs, clients et ADSS.
- Délivrance du label.
- Marketing et finances.

4.13 Procédure en cas de désaccord

Si un prestataire informatique conteste le résultat de l'audit, le cas est examiné et tranché par un second auditeur. La coordination du second 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 Guide de sécurité pratique

Il existe le «Guide de sécurité pratique» de la société isec ag. Ce guide a été élaboré indépendamment du standard, mais décrit des implémentations possibles pour atteindre les exigences du standard. Il peut être compris comme une boîte à outils. Les détails sont disponibles sur le site web suivant : https://sihb.ch.

5 Exigences d'audit

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

Chaque question de la liste de contrôle CyberSeal se voit attribuer une priorité telle que décrite au chapitre 4.4. De plus, la liste de contrôle CyberSeal définit, conformément au chapitre 4.5, quelles sections font l'objet d'une autodéclaration, d'un entretien ou d'un audit console. L'utilisation de la liste de contrôle CyberSeal garantit une réalisation homogène des audits CyberSeal et définit le standard CyberSeal actuel.

Les principaux contenus de la liste de contrôle d'audit CyberSeal sont présentés ci-après. La formulation contraignante de chaque point de contrôle peut être consultée dans la liste de contrôle.

5.1 Répartition des tâches client/prestataire informatique

La répartition des tâches entre le prestataire informatique et la PME doit être décrite par écrit et avec suffisamment de détails. La documentation doit

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

Il doit notamment être clairement défini qui est responsable de quels aspects de la sécurité.

Il n'est pas obligatoire de créer un document distinct pour chaque client. Des contrats de maintenance ou des descriptions de service peuvent être suffisants.

Le prestataire informatique établit régulièrement pour le client un rapport de sécurité dans lequel les événements de sécurité pertinents, les risques identifiés ainsi que les mesures mises en œuvre et planifiées sont documentés et évalués de manière transparente.

5.2 Gestion des accès à l'infrastructure client

Le prestataire informatique doit démontrer comment il réglemente et gère les accès à l'infrastructure client.

Les objectifs suivants doivent être atteints :

- Il doit être garanti que le client peut changer de prestataire informatique à tout moment. Un niveau de sécurité élevé est mis en œuvre pour l'accès à l'infrastructure client (authentification multifacteur). Les collaborateurs qui quittent un prestataire informatique n'ont en aucun cas accès à l'infrastructure client.
- Le client doit être conscient des informations auxquelles le prestataire informatique peut accéder.

5.3 Identifiants et droits d'accès

Les identifiants désignent généralement le nom d'utilisateur et le mot de passe. Il doit être garanti que les points suivants sont respectés :

- Un processus doit être mis en place rendant toute modification d'identifiants (y compris la réinitialisation de mots de passe) et de droits d'accès traçable. Le processus doit également couvrir les droits temporaires.

- En cas d'urgence, le client peut accéder à tous ses identifiants et droits d'accès.
- Les mots de passe du client sont stockés de manière sécurisée (ex. coffre-fort de mots de passe).

Un processus défini et sécurisé existe pour la modification des comptes, des mots de passe et des droits d'accès, garantissant que les modifications ne sont effectuées que de manière autorisée, traçable et selon le principe du besoin d'en connaître.

Un processus défini et sécurisé existe pour l'attribution et la révocation des droits temporaires, prévoyant notamment une limitation temporelle claire, une documentation et une révocation automatique de ces droits.

5.4 Documentation

Le prestataire informatique doit disposer d'une documentation à jour de l'infrastructure de la PME. Cette documentation comprend au minimum :

- Tous les systèmes sont répertoriés dans un inventaire.
- La documentation des systèmes peut être transmise au client sur demande. Aucun système particulier n'est nécessaire pour la lire.
- Le prestataire informatique met régulièrement à jour la documentation.

5.5 Architecture réseau

L'architecture réseau prend en compte les différentes zones :

- Zone bureautique
- Zone industrielle (OT), certains équipements ne pouvant pas être mis à jour peuvent s'y trouver.
- Zone publique pour les invités et les appareils personnels des collaborateurs.

Il convient de veiller à ce que les flux entre les zones soient réduits au strict minimum. Des routeurs ou équipements similaires supportant les règles correspondantes doivent impérativement être mis en œuvre.

5.6 Pare-feu

Les conditions cadres suivantes doivent être satisfaites :

- Les connexions individuelles du pare-feu n'autorisent que le trafic nécessaire. Le trafic sortant vers Internet doit également être restreint.
- Les règles du pare-feu doivent être lisibles pour un expert externe.
- Le jeu de règles doit être revu régulièrement. Toute révision effectuée doit être traçable.

5.7 WLAN

Le Wi-Fi chez le prestataire informatique et chez la PME s'appuie fondamentalement sur le concept du chapitre 5.5. Des exigences supplémentaires sont définies ci-après :

- Des mots de passe distincts et non déductibles doivent être utilisés pour chaque client.
- Un réseau Wi-Fi séparé doit être mis en place pour les appareils personnels des collaborateurs et pour les invités.
- L'authentification via des identifiants partagés ne peut être utilisée que pour les zones réseau publiques. L'accès à toutes les autres zones (conformément au chapitre 5.5) doit s'effectuer exclusivement avec des identifiants personnels.
- Seuls des mécanismes de protection à jour et sécurisés 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 mandater un autre prestataire. Cela peut être garanti en dotant le client d'un compte administrateur de secours.
- Les comptes à privilèges élevés ne sont pas utilisés pour les tâches applicatives quotidiennes.
- Les portails accessibles publiquement et les infrastructures cloud accessibles via des identifiants AD sont mis en œuvre de manière sécurisée.
- Seuls des comptes administrateurs nominatifs sont utilisés.

5.9 Durcissement des composants informatiques

Tous les systèmes et appareils clients configurés par le prestataire informatique sont durcis. Il existe généralement une liste de contrôle avec les paramètres de configuration nécessaires.

5.10 Messagerie électronique

Selon le BACS et les assureurs, une cyberattaque débute généralement 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 construite et exploitée de manière sécurisée. Une protection anti-malware est nécessaire, ainsi que la vérification de l'authenticité de l'expéditeur, ce qui peut être réalisé via SPF ou DKIM. L'accès depuis des appareils mobiles est contrôlé et restreint en conséquence.

L'infrastructure de messagerie des clients est souvent hébergée dans le cloud. La plupart des fournisseurs permettent ainsi de garantir un niveau de sécurité très élevé.

5.11 Gestion des correctifs

Un patching insuffisant et trop lent est identifié par le BACS et les assureurs comme l'une des causes principales des cyberattaques. De plus, selon les vulnérabilités présentes, celles-ci peuvent être exploitées pour une élévation de privilèges. Daher fällt diesem Punkt eine besondere Bedeutung zu.

Les exigences minimales suivantes doivent être mises en œuvre :

- La gestion des correctifs est définie dans un processus qui doit être impérativement respecté. Ce processus couvre également la gestion des correctifs pour les produits non-Microsoft. Les cycles de mise à jour sont définis de manière pertinente.
- Les exceptions à la gestion des correctifs (ex. Java pour une application ne pouvant pas être mis à jour) doivent être consignées par écrit.
- Face aux vulnérabilités majeures et critiques (ex. faille Exchange), un processus d'urgence doit obligatoirement être déclenché.

5.12 Appareils mobiles

Actuellement, les appareils mobiles ne sont pas la principale cause des incidents de cybersécurité majeurs dans les PME. Un niveau de sécurité minimal doit néanmoins être garanti.

- Les supports de données sur les appareils mobiles doivent être chiffrés 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 appliqués techniquement via des politiques. L'utilisation de

politiques peut s'avérer pertinente et efficace pour les PME.

5.13 Télétravail / Bureau à domicile

De nombreux prestataires informatiques peuvent satisfaire aux exigences de leurs clients même lorsque leurs collaborateurs travaillent à domicile. Le télétravail permet également de garantir les prestations promises en cas de pandémie.

C'est pourquoi des environnements de télétravail sécurisés sont d'une grande importance :

- Le prestataire informatique élabore et met en œuvre un concept de télétravail sûr et adapté.
- Le concept garantit qu'aucune connexion réseau directe ne peut être établie entre les systèmes clients et le domicile.
- Une forme d'authentification multifacteur doit être mise en œuvre.
- Le concept définit également les fonctionnalités complémentaires autorisées (ex. impression, mappage de lecteurs réseau, etc.).

5.14 Protection contre les logiciels malveillants

Une protection efficace contre les logiciels malveillants (antivirus) permet de prévenir de nombreuses infections. Le BACS et les assureurs accordent une grande importance à une protection anti-malware de qualité. Des tests ont montré que les nombreux produits disponibles sur le marché présentent des différences significatives. Le choix du produit utilisé est donc crucial.

La plupart des serveurs et des postes clients sont généralement assez bien protégés. De nombreuses attaques passent par le système de messagerie. Un concept de protection à deux niveaux (pare-feu et poste client) est donc impératif pour les systèmes de messagerie.

Une protection renforcée de l'accès Internet est également courante dans le contexte des PME.

Il est toujours courant que certains systèmes ne puissent pas être équipés d'une protection anti-malware. La raison doit être documentée. De plus, ces systèmes doivent être isolés au niveau réseau.

Une solution de détection et réponse sur les endpoints (EDR) est déployée. Elle permet une supervision continue des terminaux, une détection automatisée des menaces ainsi qu'une analyse et une réaction rapides aux incidents de sécurité.

5.15 sauvegarde / restauration

Le BACS et les assureurs définissent une bonne sauvegarde comme essentielle à la survie d'une entreprise en cas de cyberattaque. Lors d'une cyberattaque, les attaquants tentent souvent de rendre les sauvegardes inutilisables.

Une bonne sauvegarde joue donc un rôle essentiel. Outre une documentation adéquate, son bon fonctionnement doit être testé régulièrement. Il ne s'agit pas seulement de restaurer des fichiers individuels, mais aussi de restaurer des systèmes entiers et de vérifier leur fonctionnalité. Les environnements de virtualisation et les outils de sauvegarde actuels permettent ces tests réguliers.

Même les grandes entreprises tiennent à ce que les sauvegardes ne puissent plus être modifiées après coup. La bande magnétique comme support de sauvegarde connaît de ce fait actuellement un retour en grâce. En alternative, des supports amovibles sont utilisés dans de nombreux projets. Ceux-ci sont moins sécurisés qu'une bande, mais souvent moins coûteux.

Une copie de la sauvegarde doit être conservée dans un lieu distinct (hors site).

5.16 Gestion des changements / Gestion des incidents

L'accent de ce thème est mis sur la traçabilité, ce qui peut également s'avérer crucial en cas de cyberattaque. Le prestataire informatique s'assure que toutes les modifications apportées au système peuvent être retracées. Tous les incidents (incidents) peuvent également être retracés.

Certains prestataires informatiques de PME négligent parfois ce management. Or, on oublie souvent qu'un gain de temps considérable est possible si un incident ou une modification peut être retrouvé facilement. De plus, les systèmes supportent nativement une gestion rudimentaire des changements. Il faut toutefois les utiliser de manière systématique.

5.17 Journalisation

Chaque système offre une journalisation de bonne qualité. Il peut toutefois être nécessaire d'activer et de configurer cette journalisation. Cela peut être défini à l'aide d'une liste de contrôle (voir aussi chapitre 5.9). C'est un point important d'un SLA, qui devrait définir la durée de conservation et les valeurs à journaliser.

5.18 Monitoring/gestion des vulnérabilités

Une bonne supervision peut être très efficace pour un prestataire informatique. Le système de supervision peut soutenir ou mettre en œuvre la gestion des changements. De plus, la supervision permet de détecter de nombreuses attaques.

Une supervision proactive peut en outre détecter des cyberattaques et contribuer à l'évaluation des dommages.

L'étendue de la supervision doit être définie dans le cadre des SLA avec les clients. Les constats doivent être rapportés régulièrement au client.

Un processus de gestion des vulnérabilités est en place. Les systèmes et applications sont régulièrement analysés pour détecter des failles de sécurité. Les vulnérabilités identifiées sont évaluées, priorisées et corrigées dans le cadre de processus définis. Les enseignements de la gestion des vulnérabilités sont intégrés à la supervision et aux mesures de sécurité.

5.19 Élimination des supports de données / Suppression des données

Tout support de données contient des informations sensibles. Le prestataire informatique doit garantir que ces données ne tombent pas entre de mauvaises mains. En règle générale, le support est physiquement détruit.
Le prestataire informatique sensibilise le client à l'obligation de suppression régulière des données sur ses systèmes.

5.20 Services de tiers

Tout prestataire informatique doit aujourd'hui installer des produits tiers chez ses clients. Le client peut par exemple décider d'utiliser Office 365 ou de recourir à certains services cloud. Le prestataire informatique connaît ces produits et est en mesure de configurer un niveau de sécurité comparable à celui des services locaux.

De plus, le prestataire informatique accompagne le client dans l'utilisation sécurisée de ces produits et services. Les aspects de protection des données et de prévention des fuites de données sont particulièrement pris en compte. Le prestataire informatique informe le client sur les paramètres de sécurité recommandés et l'aide à les mettre en œuvre.

5.21 Gestion de l'intelligence artificielle

La charte collaborateur couvre également l'utilisation de l'intelligence artificielle (IA). Les collaborateurs sont informés sur l'utilisation sûre et responsable des outils d'IA. Le prestataire informatique s'assure que l'utilisation respecte les exigences de protection des données et de sécurité, et que des directives claires sur le traitement des données sensibles sont en place.

Le prestataire informatique tient à jour un inventaire des services utilisés. Celui-ci recense tous les services IT, services cloud et applications utilisés en interne et en externe. L'inventaire sert de base aux évaluations de sécurité, aux analyses de risques et au respect des exigences réglementaires.

Le prestataire informatique dispose d'une stratégie pour l'utilisation et la gestion de l'intelligence artificielle. Celle-ci définit les objectifs, le cadre et les responsabilités pour le déploiement des systèmes d'IA. Elle tient compte des aspects éthiques, juridiques et sécuritaires, et est régulièrement révisée et adaptée.

5.22 Formation du personnel

Ce point est qualifié de très critique par le BACS et les assureurs. Une grande partie des cyberattaques débute par un e-mail compromis. Chaque collaborateur doit impérativement être en mesure d'identifier les faux e-mails et d'adopter le bon comportement. C'est pourquoi les clients et les prestataires informatiques doivent être régulièrement formés. Cette formation couvre également le comportement approprié du collaborateur lors de la réception de tels faux e-mails.

5.23 Plan d'urgence

Le BACS et les assureurs considèrent l'élaboration d'un plan d'urgence comme très importante.

Un plan d'urgence garantit que tous les aspects sont couverts lors d'un événement exceptionnel et que les préparatifs nécessaires peuvent être élaborés et testés sans précipitation. Le plan d'urgence doit couvrir les événements les plus importants. La cybercriminalité représente actuellement un risque majeur (rançongiciels,

chiffrement des données, vol de données et menace de divulgation), qui doit impérativement être couverte.

Une urgence peut survenir aussi bien chez le prestataire informatique que chez ses clients. Il est donc judicieux d'élaborer au moins dans le domaine informatique un plan d'urgence compatible. Il sera nécessaire que le prestataire informatique soit intégré dans le plan d'urgence d'un client final.

Dans le domaine informatique, le plan d'urgence doit définir qui assure et comment la communication externe. Il définit également quelles instances doivent être informées pour résoudre l'urgence (police, BACS, assurances, entreprises de support, etc.). Les coordonnées correspondantes font partie intégrante du plan d'urgence.

Dans le domaine informatique, la gestion des données chiffrées doit être réglementée. Il faut s'assurer que la récupération des données est possible même en cas de défaillance d'un AD par exemple. Des tests réguliers du plan d'urgence sont importants. Ils forment les personnes clés et mettent en évidence les points faibles.

5.24 Échéances à surveiller

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

Le matériel obsolète représente un autre risque. Lorsque plus aucun correctif de sécurité n'est disponible, les composants doivent être remplacés.

5.25 Sécurité physique

La sécurité physique doit être garantie par le prestataire informatique. L'accès aux locaux du prestataire informatique doit être réglementé. L'accès aux éventuels datacenters du prestataire doit notamment être réduit au strict minimum.

Les équipements du prestataire informatique doivent être protégés de manière appropriée contre les influences extérieures (onduleur, climatisation, connexion Internet redondante, etc.).

5.26 Gestion des risques

Un prestataire informatique doit mettre en œuvre une gestion des risques pertinente. Les résultats de la gestion des risques sont documentés dans un Risk Report, signé annuellement par le conseil d'administration à l'intention de la direction ; par cette signature, les risques résiduels sont explicitement acceptés. Les risques essentiels doivent être identifiés. Ils peuvent être atténués par les mesures suivantes :

- Évitement du risque : Une analyse des risques peut conduire à la conclusion que certains services ne peuvent pas être proposés.
- Réduction du risque : Des mesures sont prises pour atténuer un risque spécifique. Tous les chapitres précédents du chapitre 5 constituent des mesures de réduction des risques.
- Transfert du risque : Certains risques peuvent être assurés. Le type d'assurance (responsabilité civile professionnelle, dommages cyber, pertes financières, etc.), le montant assuré et les prestations complémentaires (ex. assistance lors d'une cyberattaque) doivent être soigneusement choisis.
- Acceptation du risque : Toute entreprise doit assumer certains risques (ou risques résiduels). L'acceptation des risques doit impérativement être validée par la direction du prestataire informatique et ne peut pas être déléguée.

Un prestataire informatique devrait accompagner ses clients dans l'élaboration de leur propre gestion des risques. Il peut dans de nombreux cas les aider et répondre à leurs questions.

Dans le cadre de la gestion des risques IT, la résilience numérique doit être prise en compte. Celle-ci décrit la capacité du prestataire informatique à se préparer aux perturbations, incidents de sécurité ou cyberattaques, à les gérer et à rétablir rapidement les opérations. Cela comprend des mesures organisationnelles, techniques et humaines appropriées pour garantir la résilience des services et processus IT. Les enseignements des analyses de risques doivent être utilisés de manière ciblée pour renforcer la résilience numérique. Dans le cadre de la gestion des risques IT, la résilience numérique du prestataire informatique et de ses clients est systématiquement prise en compte.

5.27 Protection des données et aspects juridiques

Les exigences légales et réglementaires pertinentes (ex. LPD, LSI) sont connues et prises en compte. Le prestataire informatique identifie les réglementations applicables pour lui-même et ses clients. Il en dérive les mesures organisationnelles et techniques nécessaires.

Une analyse d'impact a été réalisée et un processus de notification obligatoire est en place. En cas d'incident de protection des données ou de sécurité, il est examiné si une notification aux autorités ou aux personnes concernées est requise. Le processus définit les responsabilités, les délais et les obligations de documentation.

Le prestataire informatique accompagne les clients, si nécessaire, dans les exigences de la LPD et de la LSI. Cela comprend les analyses d'impact, les obligations de notification et la mise en œuvre de mesures appropriées. L'objectif est une utilisation sûre et juridiquement conforme des services IT. Pour les bases légales pertinentes (en particulier la LPD et la LSI), une analyse d'impact a été réalisée, et un processus défini existe pour satisfaire aux éventuelles obligations de notification.

5.28 Développement logiciel

Un processus est en place et les principes fondamentaux du développement logiciel sécurisé (ex. OWASP Top 10) sont appliqués de manière systématique. Le prestataire informatique intègre ces principes dans toutes les phases du développement. Cela comprend des formations, des listes de contrôle et des vérifications automatisées.

Les entrées utilisateur sont correctement traitées pour prévenir les attaques de type injection SQL ou cross-site scripting (XSS). La validation, l'échappement et les requêtes paramétrées sont des standards. Le prestataire informatique vérifie cela systématiquement lors des revues de code et des tests.

Les aspects de sécurité sont intégrés dans le processus de revue de code afin d'identifier et de corriger les vulnérabilités au plus tôt. Chaque revue comprend une vérification de sécurité selon des critères établis. Les écarts requièrent une approbation et une correction.

Un processus est mis en œuvre pour vérifier que les fichiers journaux et les messages d'erreur ne divulguent pas d'informations sensibles. La journalisation est réalisée de manière sécurisée et anonymisée. Des vérifications régulières assurent la conformité.

Le développeur utilise systématiquement des outils et tests de sécurité (ex. analyse statique/dynamique, tests d'intrusion) pour identifier les vulnérabilités. Cela est ancré dans le processus de développement. Les résultats sont documentés et corrigés.

Comité des auditeurs de l'Alliance pour la Sécurité Numérique Suisse

6 Annexe

Liste des abréviations

ADSS	Allianz Digitale Sicherheit Schweiz ADSS
BACS	Office fédéral de la cybersécurité
BSI	Office fédéral allemand de la sécurité des technologies de l'information
Cobit	Control Objectives for Information and Related Technology
DKIM	DomainKeys Identified Mail
IEC	International Electrotechnical Commission
IKT	Informations- und Kommunikationstechnik
ISO	Internationale Organisation für Normung
PME	Petite(s) et Moyenne(s) Entreprise(s)
NCSC	National Cyber Security Center
NIST	National Institute of Standards and Technology
SLA	Service Level Agreement
SPF	Sender Policy Framework

Abréviations liste de contrôle

HA	écart majeur
NA	écart mineur
NV	Non disponible / non vérifiable
HW	Hinweis
KD	Kunden Infrastruktur
EG	Eigene Infrastruktur / Infrastruktur des IT- Dienstleisters
S	autodéclaration
I	Interview
K	Konsolen Audit