Redguard

Security Survey

2021

REDGUARD
SECURING YOUR ASSETS

Avec la publication de la norme minimale pour les TIC[1] par la Confédération, la Suisse dispose depuis 2018 d'une spécification uniforme et intersectorielle en matière de protection contre les risques cyber. Mais quel est exactement le niveau de sécurité actuel en Suisse? Est-il nécessaire d'agir ou les organisations et entreprises suisses disposent-elles déjà d'un niveau de sécurité suffisant? Ces questions trouvent leur réponse dans l'enquête Redguard Security Survey 2021.

Pour la troisième année consécutive, Redguard AG publie les résultats de son enquête sur la norme minimale pour les TIC. Cette année encore, nous avons écrit à plus de 1000 organisations pour leur demander de procéder à une auto-évaluation de leur niveau de sécurité actuel. Pour ce faire, nous avons développé un Quick-Test de la norme minimale pour les TIC (www.ikt-redguard.ch).

Il existe encore un grand nombre d'organisations insuffisamment préparé face aux incidents de cybersécurité. Selon les entreprises participantes à l'enquête, les mesures préventives et réactives ne sont pas suffisamment prises en compte. Près de deux tiers des organisations interrogées ont déclaré être mal préparées face à un incident (p.ex. disposant d'un plan de gestion des incidents (Incident Management Plan) ou un plan de continuité des activités (Business Continuity Plan).

Il est impossible d'atteindre un état de sécurité de l'information stable car il s'agit d'un processus qui doit être vécu, revu et développé en permanence. Il faut donc se rendre à l'évidence: aucune organisation n'est armée à cent pour cent contre les risques cyber et un incident peut toujours survenir même lorsque toutes les précautions sont prises. S'y préparer en faisant des sauvegardes et en testant régulièrement leur récupération est un premier pas dans la bonne direction. Chaque organisation doit toutefois aussi se pencher sur la meilleure manière de réagir concrètement en cas d'incident (Incident Management) et sur la façon de maintenir les processus qui peuvent encore l'être (Business Continuity Management). L'année écoulée nous a montré qu'une préparation inadéquate à un incident peut être déterminante pour la pérennité d'une organisation. Swiss Windows AG, par exemple, a dû déposer son bilan après qu'une attaque ransomware ait entraîné un arrêt de la production[2]. Parce qu'un tel cas ne doit pas être une fatalité, l'Office fédéral pour l'approvisionnement économique du pays (OFAE) a publié la norme minimale pour les TIC. Celle-ci permet à une organisation de se protéger et de prévenir les incidents, mais aussi de développer un système grâce auquel elle peut rendre ses processus de base aussi résilients que possible (Business Continuity Management) et restaurer rapidement les systèmes affectés.

Nos plus vifs remerciements pour votre coopération
Votre équipe Redguard

[1] Norme minimale de l'Office fédéral pour l'approvisionnement économique du pays (OFAE) pour les TIC (technologies d'information et de communication): https://www.bwl.admin.ch/bwl/fr/home/themen/ikt/ikt_minimalstandard.html

[2] SRF: https://www.srf.ch/news/regional/ostschweiz/konkurs-fensterhersteller-offenbar-zwang-eine-cyberattacke-swisswindows-in-die-knie

Retour d'information sur le Quick-Test de la norme minimale pour les TIC

Les résultats de l'enquête Redguard Security Survey sont basés sur une auto-évaluation des entreprises. Avec ce test rapide, les entreprises et organisations ont l'occasion d'évaluer leur niveau de sécurité en un temps record et de prendre les mesures qui s'imposent sur cette base.

Le Quick-Test de la norme minimale pour les TIC développé par Redguard comporte dix questions qui ciblent les éléments essentiels de ladite norme. Les thèmes abordés sont les suivants: Gestion des risques, Stratégie de cybersécurité, Sensibilisation & Formation, Surveillance des systèmes, Gestion des incidents (Incident Management), Gestion de la continuité des activités (Business Continuity Management), reprise après sinistre (Disaster Recovery) et Communication de crise.

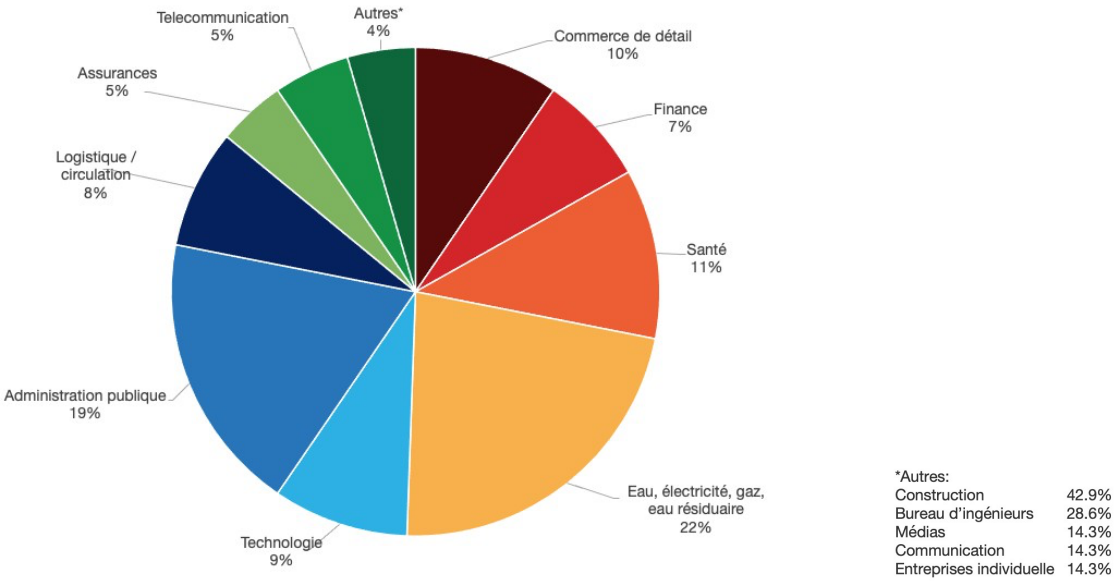


Figure 1: Entreprises interrogées par branche (%)

Redguard a invité plus de 1000 organisations suisses à évaluer leur niveau de sécurité au moyen du Quick-Test de la norme minimale pour les TIC. Cette année encore, elles s'y sont intéressées en nombre (179 organisations de différentes branches) et nous ont fourni leur auto-évaluation.

La figure 1 montre que la base sur laquelle l'enquête Security Survey repose est solide. Les entreprises et organisations participantes proviennent d'une grande variété de branches, y compris du secteur public. Parallèlement, les entreprises de tailles diverses ont contribué à l'enquête Security Survey (cf. Figure 2). Selon les données qu'elles ont fournies, 22% d'entre elles sont de grandes entreprises de plus de 500 employés. Les quelques 80% restantes se répartissent de manière plus ou moins équilibrée, avec 40% de petites entreprises (1-50 employés) et 38% de moyennes entreprises (50-500 employés).

Figure 2: Entreprises interrogées par nombre d'employés

La majorité des organisations ne respectent pas la norme minimale pour les TIC

Le niveau de sécurité évalué par les quelques 180 organisations interrogées est encore bien en deçà du niveau minimum recommandé par la Confédération et les associations en 2021. Par rapport aux années précédentes, certaines valeurs se sont même encore détériorées, ce qui indique qu'une grande partie des entreprises (en particulier les PME) ne sont pas en mesure de mettre en œuvre la norme minimale pour les TIC sans le soutien de partenaires externes tels que Redguard.

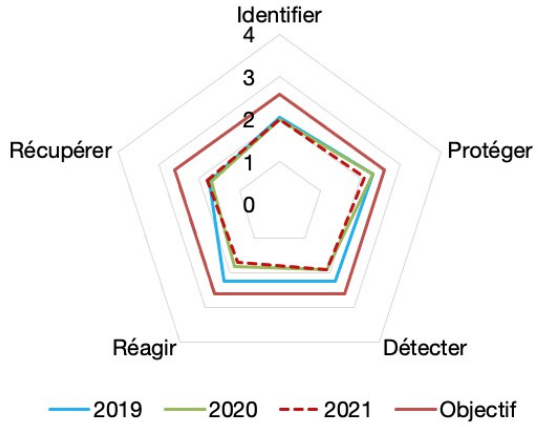


Figure 3: Résultats de l'enquête Redguard Security Survey

	2019	2020	2021	Objectif
Identifier	2.0	2.0	2.0	2.6
Protéger	2.3	2.3	2.1	2.6
Détecter	2.2	1.9	1.9	2.6
Réagir	2.2	1.8	1.7	2.6
Récupérer	1.7	1.7	1.8	2.6

Tableau 1: Résultats en chiffres par rapport à l'année précédente

La figure 3 montre que, selon leur propre évaluation, la majorité des organisations interrogées n'ont pas encore atteint le niveau de sécurité minimal de la norme minimale pour les TIC.

Fonction	Non atteint	Atteint
Identifier	62%	38%
Protéger	55%	45%
Détecter	63%	37%
Réagir	71%	29%
Récupérer	70%	30%
Total	64%	36%

Tableau 2: Résultats de l'enquête Security Survey selon les cinq fonctions

Un examen des réponses (Tableau 2) ventilées selon les cinq fonctions de la norme minimale pour les TIC montre clairement que seules 36% des organisations considèrent qu'elles atteignent le niveau de sécurité requis.

Ce qui est frappant ici, c'est que les entreprises se classent nettement mieux pour les fonctions Identifier, Protéger et Détecter que pour les fonctions Réagir et Récupérer.

Cela peut s'expliquer par le fait que les incidents liés aux ransomwares ont montré, premièrement, l'existence d'une marge de progression importante dans la réponse appropriée aux incidents de cybersécurité et, deuxièmement, l'importance des plans de réaction et de récupération.

Par ailleurs, on constate que le niveau de sécurité a stagné, et s'est même continuellement détérioré au cours des deux dernières années. Ainsi, comme le montre le tableau 1, les fonctions Protéger, Détecter et Réagir se sont dégradées au cours des deux dernières années, tandis que les capacités à Récupérer se sont légèrement améliorées et que les capacités à Identifier sont restées identiques. Il apparaît donc que les organisations (en particulier les PME) ne sont pas à même de mettre en œuvre la norme minimale pour les TIC de manière indépendante, et qu'elles dépendent pour cela d'un soutien externe, comme par exemple de la part de Redguard.

Nombre d'entreprises ne sont pas encore suffisamment préparées aux situations d'urgence

L'enquête Redguard Security Survey montre que la majorité des entreprises participantes ne sont pas suffisamment préparées face à un incident de cybersécurité. Une grande partie d'entre elles a indiqué ne pas disposer d'un processus de gestion des incidents de cybersécurité totalement opérationnel (65%).

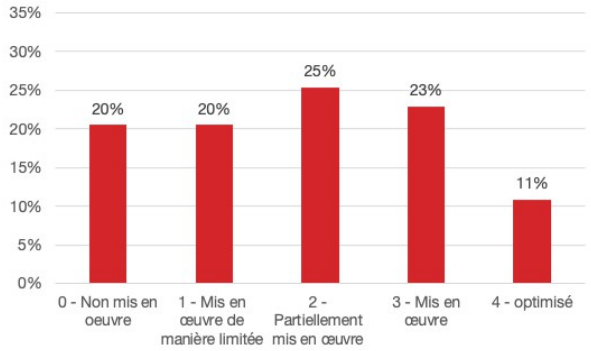


Figure 4: Processus de gestion des incidents de cybersécurité (Incident Management)

Sans un processus approprié, il est peu probable que les incidents de cybersécurité puissent être détectés, contenus et les dommages qui en résultent réparés en temps utile. Cela est confirmé par le fait que, ici aussi, une majorité d'organisations déclarent être mal préparées à des incidents importants (75%).

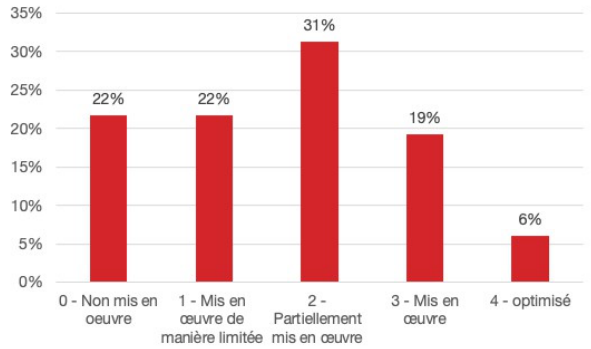


Figure 5: Gestion définie et testée de la reprise après sinistre (Disaster Recovery) et de la continuité des processus (Business Continuity)

Il ressort de leurs déclarations que les plans de Disaster Recovery et de Business Continuity font totalement défaut ou, s'ils existent, ne sont pas régulièrement testés. Cela signifie que beaucoup de temps est perdu en cas d'urgence car il faut d'abord clarifier les responsabilités et les compétences, alerter les bonnes personnes et mettre sur pied les mesures à prendre. Il en va de même pour la communication de crise. Moins d'un tiers seulement des organisations participantes disposent d'un plan de communication (28%).

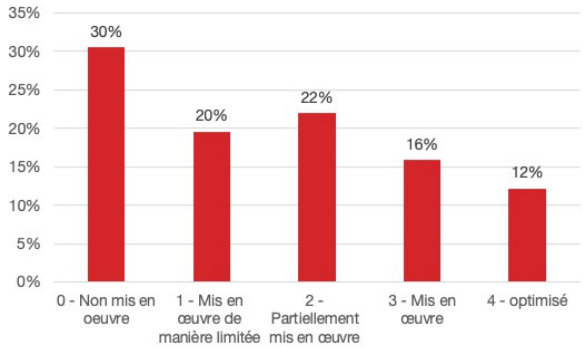


Figure 6: Existence d'un plan de communication

En cas d'absence de plan de communication, un incident de cybersécurité peut rapidement se transformer en crise. L'absence de réaction ou de communication implique souvent une culpabilité et encourage la propagation de rumeurs (mots clé: médias sociaux et médias en ligne).

Au contraire, une communication honnête, rapide et factuelle peut avoir un effet de désescalade en cas de crise. Elle peut également servir à gérer l'image publique de sa propre organisation en cas d'incident.

Un processus défini, associé à des plans de Disaster Recovery et de Business Continuity, est une condition préalable à la gestion réussie des incidents de cybersécurité. Si cela s'accompagne en outre d'une communication active et honnête, il est possible de limiter les dommages causés à l'image de l'entreprise. Dans l'idéal, une gestion compétente de la crise lors d'un incident de cybersécurité conduit même à donner une image positive de l'organisation aux partenaires et clients.

Redguard vous aide à vous conformer à la norme minimale pour les TIC

La norme minimale pour les TIC est conçue de manière à pouvoir être mise en œuvre par toutes les entreprises, quelle que soit leur branche ou leur taille. Les lignes directrices et l'outil d'auto-évaluation de l'Office fédéral pour l'approvisionnement économique du pays[3] présupposent de solides connaissances spécialisées et une approche pragmatique est indispensable pour réussir à implémenter la norme minimale pour les TIC. Redguard apporte son expertise aux entreprises à cet égard.

Identifier: Connaissez vos risques et adoptez une approche stratégique de la sécurité de l'information

- Redguard vous aide à identifier les risques cyber de votre organisation et à les répertorier de manière systématique. Ensemble, nous mettons sur pied une stratégie de sécurité de l'information basée sur vos risques afin de les gérer et de les contrôler.

Protéger: Protégez vos systèmes et formez vos employés

- Élaborez des directives pour protéger vos systèmes et mettez-les en œuvre. Redguard vous aide à élaborer les bonnes mesures dans les domaines de la gestion des accès, de concept Firewall, de concept de zone réseau ainsi que de la protection contre les Malwares.
- Les mesures techniques ne suffisent souvent pas: formez vos employés et montrez-leur comment ils peuvent contribuer à sécuriser les informations. Redguard vous apporte son soutien, soit à l'aide d'offres de formation classiques, soit par des campagnes de Live Hacking ou de phishing.

Détecter: Connaissez vos points faibles et testez votre défense

- Mettez en place vos systèmes et processus de sorte que les incidents de sécurité potentiels puissent être détectés.
- Mettez vos systèmes et votre sécurité informatique à l'épreuve en effectuant des tests de pénétration ou de simulation d'attaque. Les spécialistes de Redguard effectuent des tests et des attaques ciblées en votre nom afin d'identifier les opportunités d'amélioration.

Réagir: Planifiez et pratiquez votre réaction aux incidents de cybersécurité

- Un plan de réponse vous aide à réagir correctement en cas d'urgence et à gagner du temps. Lorsqu'un plan de réaction est en place, vous avez déjà répondu à de nombreuses questions: Qui est responsable dans votre organisation en cas d'incident de cybersécurité? Comment informez-vous vos employés et vos clients? Fermez-vous complètement les systèmes ou maintenez-vous un fonctionnement d'urgence de certaines activités?
- Chez Redguard, vous pouvez vous entraîner à gérer un cas d'urgence à l'aide d'un exercice Tabletop. Jouez un scénario adapté à votre organisation, étape par étape, et tirez-en des opportunités d'amélioration et des mesures à prendre.

Récupérer: Retour à la normale

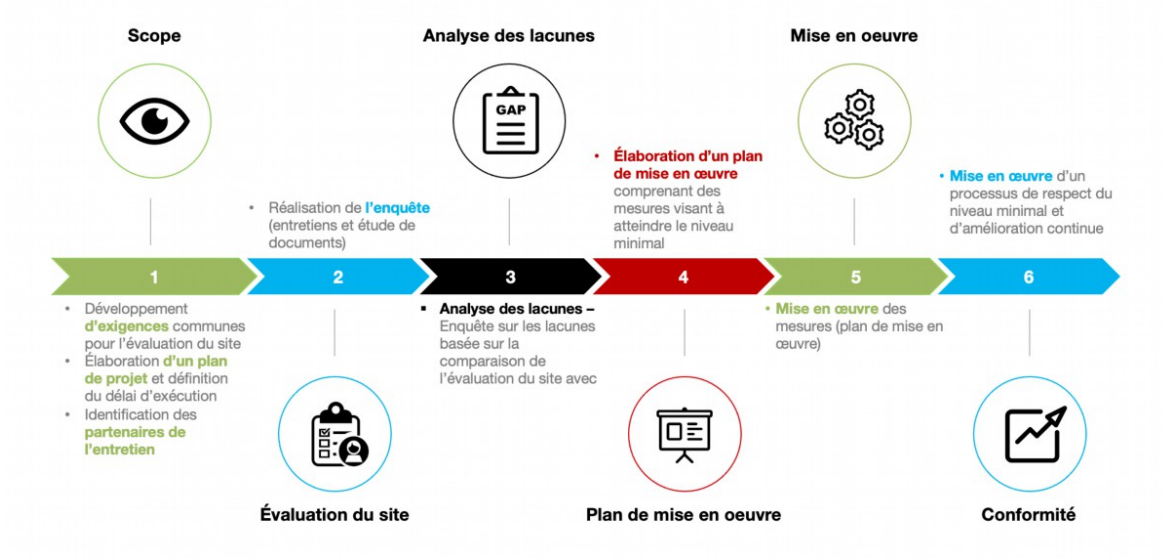
- Établissez un plan de récupération et fixez des objectifs de récupération spécifiques: Pour quelle durée maximum pouvez-vous vous passer de vos systèmes? Combien de pertes de données pouvez-vous supporter?
- Redguard aide votre organisation à atteindre le niveau minimum de sécurité recommandé dans la fonction «Récupérer» en travaillant avec vous pour développer des plans de récupération.

---

[3] Norme minimale pour les TIC (technologies d'information et de communication) de l'Office fédéral pour l'approvisionnement économique du pays (OFAE): https://www.bwl.admin.ch/bwl/fr/home/themen/ikt/ikt_minimalstandard.html

Mise en œuvre globale de la norme minimale pour les TIC

Concentrez-vous sur votre activité principale, pendant que nous faisons passer votre sécurité informatique au niveau supérieur. Avec une équipe de plus de 50 spécialistes de la sécurité, nous vous offrons des services complets.



Évaluation du site selon la norme minimale pour les TIC

Faites déterminer le degré de maturité de votre sécurité de l'information par un organisme indépendant. Nos spécialistes vérifient vos systèmes, documents et processus. Les résultats obtenus sont discutés plus en détail dans le cadre d'entretiens. Au final, vous recevez un rapport énumérant les vulnérabilités qui ont été identifiées et les mesures et recommandations d'action concrètes pour y remédier et améliorer la sécurité des informations.

CISOaaS – Mise en œuvre et maintien de la norme minimale pour les TIC

Avec le service «Security Officer as a Service» (SOaaS), vous avez un interlocuteur personnel qui met à votre disposition tout le savoir-faire de Redguard. Cette personne agit en tant que chef de projet au sein de votre organisation pour appliquer les recommandations d'actions issues de l'évaluation du site. Ce faisant, elle garantit le maintien de la norme minimale pour les TIC et l'amélioration continue du degré de maturité.

Soutien en cas de «Worst Case»

Si, malgré toutes les mesures prises, votre entreprise est touchée par un incident de cybersécurité, les spécialistes de Redguard sont toujours disponibles pour vous aider.

Annexe 1: Présentation du Quick-Test

Le Quick-Test développé pour cette étude est basé sur les cinq fonctions de la norme minimale pour les TIC et comporte dix questions spécifiques. Cela permet de se prononcer sur le niveau de maturité des organisations interrogées. Vous trouverez le Quick-Test à l'adresse suivante:

http://ikt.redguard.ch

N°	Question
1	**Risques et vulnérabilités (Identifier)** (J'étudie les risques et les vulnérabilités et j'identifie les systèmes critiques)
2	**Stratégie de cybersécurité (Identifier)** (J'ai émis des directives pour la cybersécurité dans mon entreprise, par exemple sous la forme d'une stratégie et d'une politique/de directives)
3	**Politique & Processus (Protéger)** (Je fixe une politique pour la protection des systèmes d'information et des ressources, y compris un processus d'amélioration continue et de développement de la sécurité de l'information)
4	**Sensibilisation & Formation (Protéger)** (Je m'assure que tous les employés de notre organisation sont formés à la sécurité de l'information, à chaque niveau et pour chaque fonction, et qu'ils connaissent leurs responsabilités et le comportement à adopter)
5	**Détection/Monitoring (Détecter)** (Je mets en place un monitoring continu des systèmes et des réseaux pour détecter les incidents potentiels de cybersécurité)
6	**Détection/Contention (Détecter)** (Je définis le processus pour m'assurer que l'on détecte à temps les anomalies et les incidents de sécurité et que l'on comprenne l'impact potentiel d'un incident)
7	**Mon organisation est prête à faire face à des incidents majeurs (Réagir)** (J'ai développé et testé régulièrement un processus pour répondre aux incidents qui se produisent – par exemple Business Continuity Management, Incident Response Planning, Disaster Recovery)
8	**Processus de gestion des incidents (Réagir)** (Je veille à ce que les incidents de cybersécurité puissent être contenus et à ce que leur propagation soit stoppée afin que leur impact soit atténué)
9	**Planification de la récupération (Récupérer)** (Je m'assure que j'ai mis en place un plan de récupération qui garantis le rétablissement rapide des systèmes après un incident)
10	**Plan de communication (Récupération)** (J'ai préparé un plan de communication en cas d'incident de cybersécurité et je m'assure qu'il tient compte de l'image de mon organisation auprès du public)

Annexe 2: Présentation de l'échelle de maturité

Chacune des dix questions du Quick-Test est notée sur une échelle de 0 à 4. Pour chacune des cinq fonctions (Identifier, Protéger, Détecter, Réagir et Récupérer), le niveau de maturité est déterminé par la moyenne des scores obtenus aux deux questions.

Niveau	Réponse
0 – Non mis en œuvre	Ce point serait important pour mon organisation, mais jusqu'à présent il n'existe que très peu d'informations à ce sujet.
1 – Mis en œuvre de manière limitée	Le processus/la directive n'est pas entièrement définie et n'est pas approuvée.
2 – Partiellement mis en œuvre	Le processus/la directive est presque entièrement définie et acceptée, mais déjà quelque peu dépassée, au moins en partie.
3 – Mis en œuvre	Le processus/la directive est entièrement définie et en grande partie approuvée. Il/elle est également relativement récente et toujours valable et correcte. Toutefois, cette approche est largement statique.
4 – Optimisé	Le processus/la directive est entièrement mise en œuvre. Il/elle est revue en permanence, améliorée régulièrement et son efficacité est assurée.

Pour en savoir plus sur la norme minimale pour les TIC:

- Quick Test
  http://ikt.redguard.ch
- Site web de l'Office fédéral pour l'approvisionnement économique du pays
  https://www.bwl.admin.ch/bwl/fr/home.html
- Téléjournal du 27.08.2018 (en allemand)
  https://www.srf.ch/news/schweiz/cyber-angriffe-auf-unternehmen-ein-minimalstandard-fuer-minimalen-schutz
- Factsheet Redguard (en allemand)
  https://www.redguard.ch/downloads/factsheet_ikt_minimalstandard_de.pdf
- Site web de Redguard
  https://www.redguard.ch/