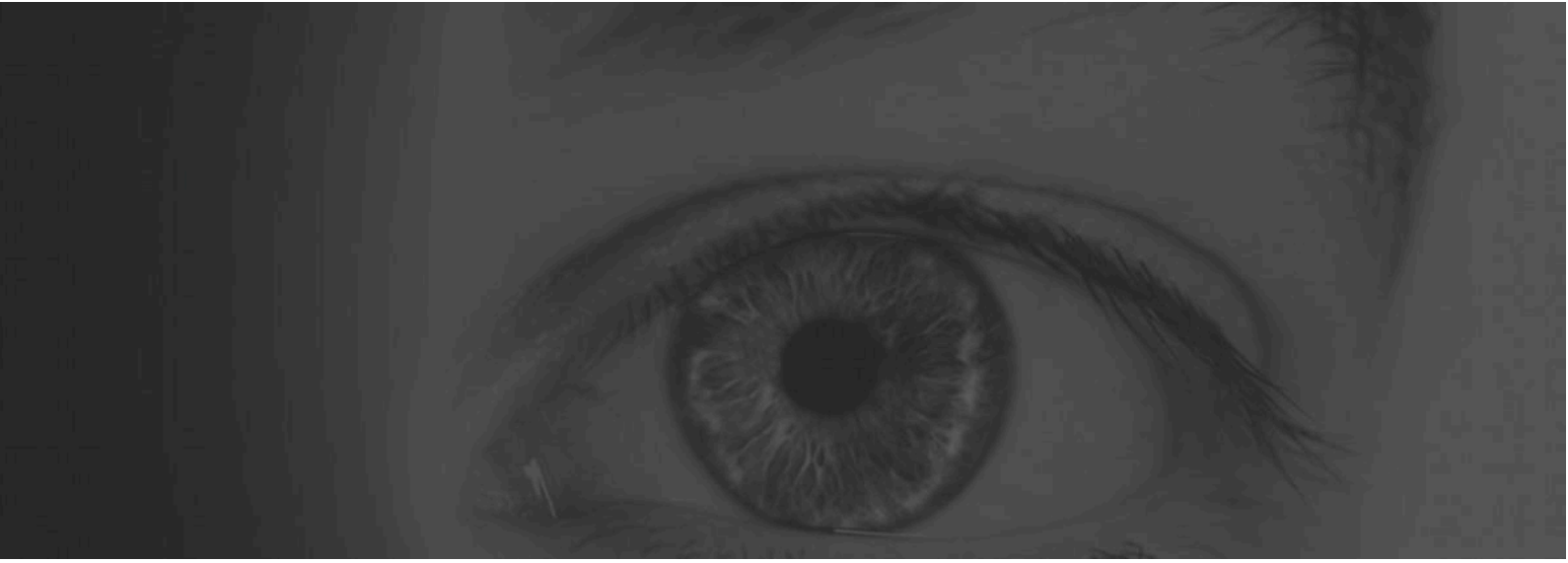


Redguard

Security Survey

2024

REDGUARD
SECURING YOUR ASSETS

Découvrez comment le niveau de cybersécurité des organisations et des entreprises suisses a évolué au cours des six dernières années. Les résultats sont basés sur la norme minimale en matière de TIC et couvrent entre autres des éléments clés importants tels que la gestion des risques, la gestion des fournisseurs, la sensibilisation et la formation, la surveillance et la gestion des logs, la gestion des incidents, la gestion de la continuité des activités et la communication de crise. Les entreprises participantes ont évalué leur niveau de sécurité actuel à l'aide de notre Quick-Test de sécurité. Découvrez quelles sont les mesures les plus appropriées au vu des résultats obtenus.

L'enquête de sécurité de Redguards pour la sixième année consécutive

Avec la publication de la norme minimale pour les TIC par la Confédération, la Suisse dispose depuis 2018 d'une norme uniforme et intersectorielle pour la protection contre les cyberrisques. Le respect de cette norme est désormais de plus en plus une exigence pour les exploitants d'infrastructures critiques. Mais qu'en est-il du niveau de sécurité actuel des entreprises suisses ? Pour la sixième fois déjà, Redguard AG publie les résultats de son enquête basée sur la norme minimale TIC : il est temps de faire le point.

La cybersécurité, une question de leadership

Les résultats de l'enquête et les différents entretiens avec les clients nous permettent de constater que le thème de la cybersécurité a considérablement gagné en importance au cours de ces dernières années et qu'il a également atteint les niveaux de direction des entreprises. C'est ce que montre également le nouveau volet de l'enquête de cette année, à savoir le **soutien au management**. Il est réjouissant de constater que près de 80% des entreprises interrogées ont indiqué que le thème de la cybersécurité bénéficie du soutien total de la direction. Seuls 2 % d'entre elles ne ressentent encore que peu de soutien de la part de la direction.

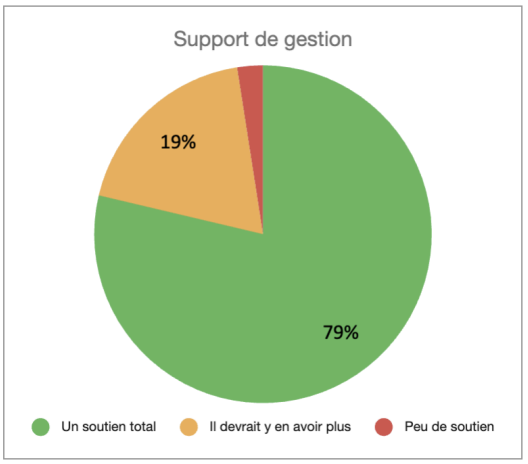


Figure 1: Le soutien de la direction est-il disponible?

Près de deux tiers des entreprises ressentent également ce soutien dans leur porte-monnaie et indiquent qu'elles disposent d'un budget suffisant pour la cyberrésilience. 33% estiment que le budget dont elles disposent est insuffisant.

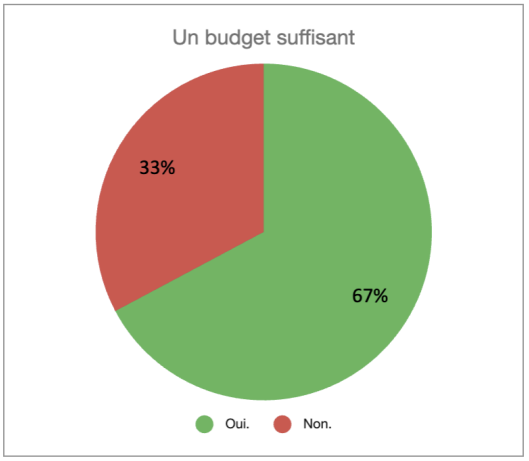


Figure 2: Le budget de sécurité disponible est-il suffisant?

Focus sur la gestion des fournisseurs et le BCM

L'année dernière, deux thèmes principaux se sont imposés dans le travail avec nos clients. D'une part, le thème de **la gestion des fournisseurs** a été largement

thématisé dans les médias par un exemple connu et, d'autre part, la nouvelle loi sur la protection des données lui a donné une importance supplémentaire. Dans quelle mesure les données de notre entreprise sont-elles protégées en cas de traitement par des tiers ? Est-ce que je sais quelles parties externes accèdent à mon infrastructure, quand et pour quelle raison ? Ces questions, que nous rencontrons de plus en plus souvent dans notre travail quotidien de conseil, ont donc été abordées dans la dernière enquête.

Les situations de crise telles que la pandémie Corona ou la multiplication des attaques de ransomware montrent qu'un **événement rare et avec un fort impact** peut se produire et qu'il est tout à fait judicieux de réfléchir à l'avance à la manière dont les **principaux processus commerciaux** peuvent être maintenus, par exemple en cas de panne à grande échelle de l'infrastructure informatique. L'enquête a également permis de déterminer dans quelle mesure des **mesures de résilience existent à cet égard** sous la forme de plans de réaction et de restauration

Security Quick Check Redguards

Les résultats des enquêtes de sécurité de Redguard se basent sur une auto-évaluation des entreprises et organisations participantes. Grâce au Quick Test, celles-ci ont la possibilité d'évaluer rapidement leur niveau de sécurité et de prendre des mesures de protection supplémentaires sur cette base.

Le Quick Test basé sur la norme minimale pour les TIC développé par Redguard se compose de 13 questions. Il couvre l'inventaire, la gestion des risques, la gestion des fournisseurs, l'accès à distance, la sensibilisation et la formation, la surveillance et la gestion des journaux, la gestion de la continuité des activités et la communication de crise.

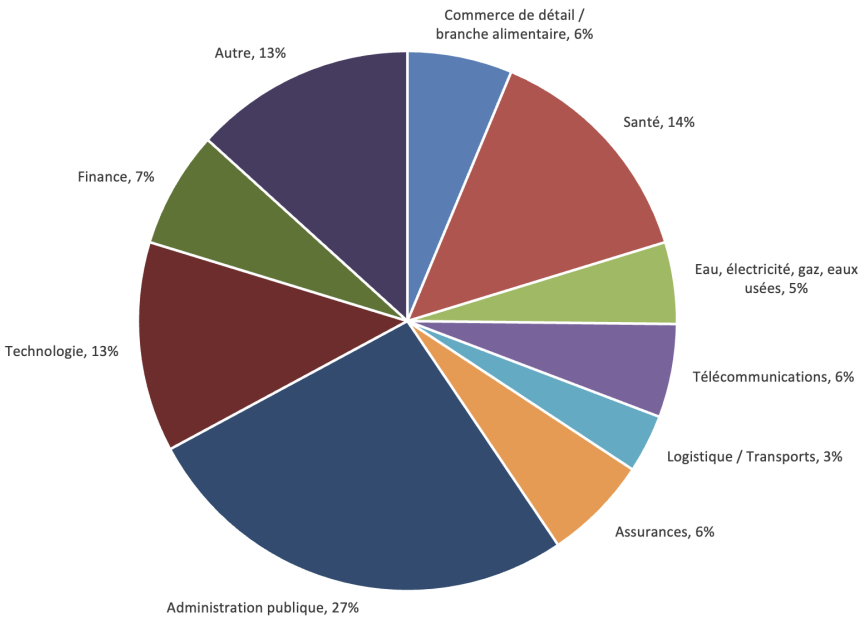


Figure 3 : Entreprises interrogées par secteur d'activité (%)

Organisations participant à l'enquête

Redguard a invité environ 2 000 organisations suisses à évaluer leur niveau de sécurité au moyen d'un test rapide sur la norme minimale pour les TIC. Cette année encore, plus de 100 organisations de différents secteurs se sont intéressées à la norme et ont rempli une auto-évaluation. La figure 3 montre que les résultats de l'enquête de sécurité sont une nouvelle fois largement étayés. Les entreprises et organisations participantes proviennent des secteurs les plus divers, avec une représentativité très équilibrée. Des entreprises de tailles très diverses ont contribué au Redguard Security Survey, comme nous pouvons le voir sur la figure 4. Selon les indications des participants, 33% d'entre elles sont de grandes entreprises de plus de 500 collaborateurs.

La plus grande partie est constituée de PME, avec 27% de petites entreprises (1 à 50 employés) et 27% de moyennes entreprises (50 à 200 employés).

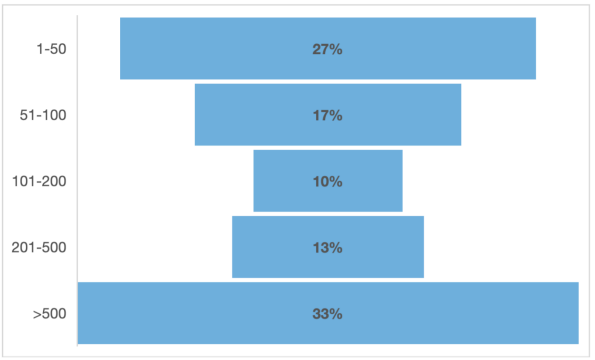


Figure 4 : Entreprises interrogées selon le nombre d'employés

Norme minimale pour les TIC - niveau de maturité accru

Dans le cadre de l'enquête de cette année, les participants ont évalué leur niveau de maturité sur l'ensemble des cinq fonctions à un niveau nettement plus élevé que l'année dernière. Certes, avec 2,4, le score global de toutes les entreprises se situe toujours en dessous de la valeur minimale "non officielle" de 2,6, mais une nette augmentation du niveau de maturité a pu être constatée par rapport à l'année précédente (score = 2,1).

Comme les années précédentes, c'est la fonction "Protéger" qui a obtenu le score le plus élevé (2,8). La mise en œuvre de mesures de sécurité techniques semble donc être beaucoup plus facile pour les personnes interrogées que les thèmes relativement liés aux processus et à l'organisation, par exemple le BCM (récupérer) ou la gestion des risques (identifier). Dans l'ensemble, la tendance à la hausse de la maturité en matière de cybersécurité dans les entreprises suisses se poursuit de manière réjouissante.
Un coup d'œil sur les réponses (tableau 1), réparties selon les cinq fonctions de la norme minimale pour les TIC, montre que seuls 41% des organisations estiment atteindre ou même dépasser le niveau de sécurité requis par la norme minimale TIC.

Fonction	2019	2020	2021	2022	2023	2024
Identifier (ID-Identify)	2.0	2.0	2.0	2.1	2.2	2.4
Protéger (PR-Protect)	2.3	2.3	2.1	2.1	2.3	2.8
Détecter (DE-Detect)	2.2	1.9	1.9	2.1	2.1	2.5
Réagir (RS-Respond)	2.2	1.8	1.7	1.9	2.1	2.3
Récupérer (RC-Recover)	1.7	1.7	1.8	2.0	2.0	2.1
Niveau de maturité	**2.1**	**1.9**	**1.9**	**2.0**	**2.1**	**2.4**

Tableau 1 : Résultats en chiffres en comparaison annuelle

Depuis des années, la fonction "Récupérer" est en queue de peloton en ce qui concerne le niveau de maturité. On peut spéculer sur les raisons possibles de cette situation, mais les expériences faites dans les projets clients de Redguard ont montré que les entreprises ont longtemps repoussé le thème de la gestion de la continuité des activités (BCM) en raison de sa complexité.

Ce n'est que ces derniers mois que l'on constate un intérêt accru pour les thèmes liés à la gestion des urgences et des crises. Dans le domaine du rétablissement, le fait que d'éventuels tests de reprise demandent beaucoup de temps et de ressources et ne peuvent donc souvent pas trouver leur place dans le budget annuel constitue un facteur aggravant.

Dans le domaine "Réagir" également, la majorité des personnes interrogées s'estiment trop peu préparées. Redguard a reconnu ce besoin et accompagne les clients d'une part dans la préparation aux incidents dans le cadre de mandats CISOaaS et, depuis bientôt deux ans, sous la forme d'un Incident Response Team qui est à vos côtés en cas de cyberattaque et peut vous apporter un soutien précieux.

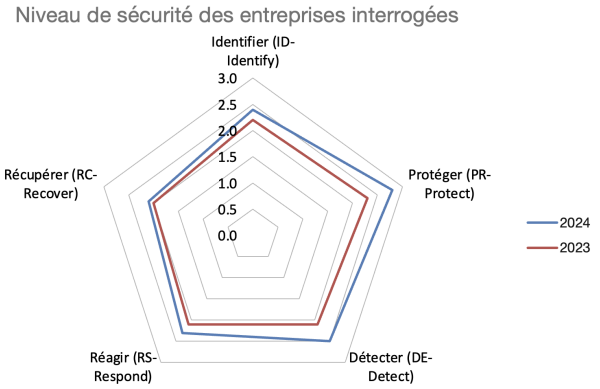


Figure 5 : Résultats de l'enquête de sécurité Redguard

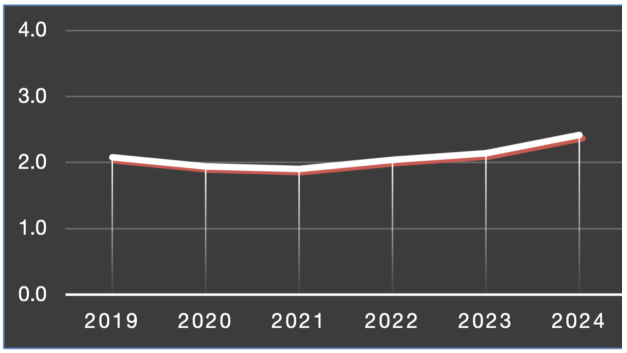


Figure 6 : Evolution du niveau de maturité et comparaison avec l'année précédente

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 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 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

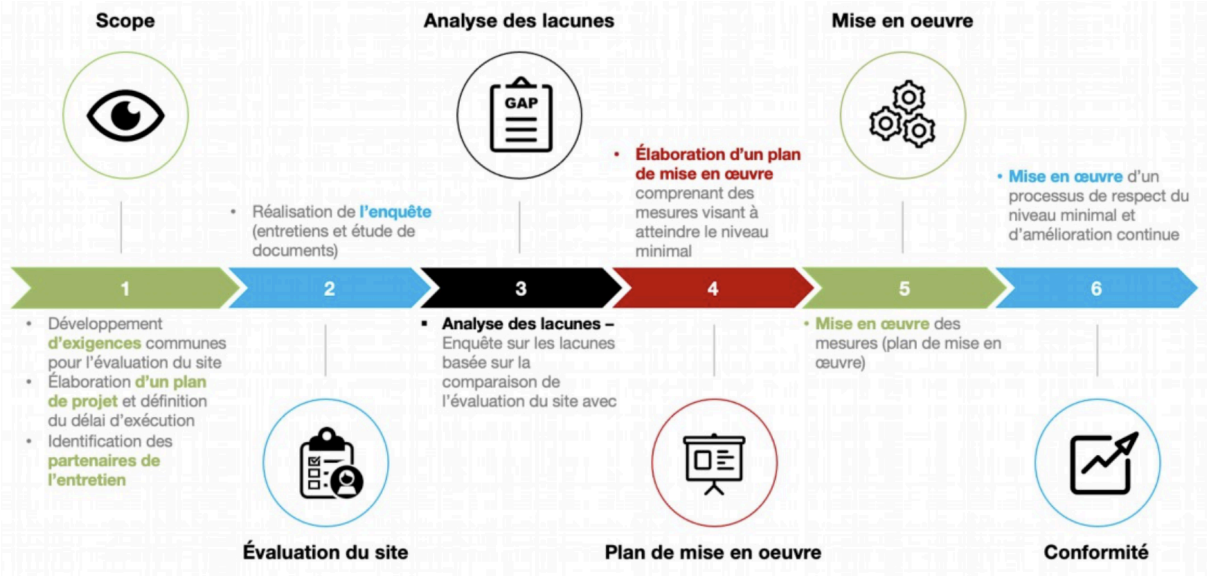
- Un plan de réponse vous aide à réagir correctement en cas d'urgence et à gagner du temps. Lorsqu'un plan de réaction est en place, vous avez déjà répondu à de nombreuses questions: Qui est responsable dans votre organisation en cas d'incident de cybersécurité? Comment informez-vous vos employés et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

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 de votre entité 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 de l'information.

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.

Aide en cas d'incident

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.

Mesures

1.1 Mesures – Opérations de sécurité (Security Operations Center, SOC)

Les opérations de sécurité se réfèrent au processus de surveillance, de vérification et de réaction aux événements de sécurité et aux menaces dans une infrastructure informatique. Elles permettent d'améliorer considérablement la cybersécurité d'une entreprise. Il s'agit avant tout de détecter et d'arrêter à temps les activités inhabituelles et potentiellement dommageables.

SOC as a Service

Avec notre Security Operations Center basé sur le cloud, vous externalisez votre cybersécurité aux experts Redguard de notre société sœur FusionOne. L'offre de services est accessible à toutes les organisations et entreprises qui utilisent Microsoft 365. Le SOC a également été développé et testé avec des PME et répond à leurs besoins au quotidien et à leur budget.

Pour plus d'informations: https://www.fusionone.ch

1.2 Mesures – Scan continu de sécurité (Continuous Security Scanning)

Grâce à des scans de vulnérabilité permanents et automatisés, vous garantissez à votre entreprise un niveau de sécurité toujours suffisant. Le Continuous Security Scanning convient pour faire le pont entre les tests d'intrusion réguliers.

Vérification automatisée des vulnérabilités

La plateforme suisse Vulnerability Guard développée par Redguard vous permet d'évaluer au mieux votre niveau de sécurité et de replacer les données dans un contexte historique. Vous pouvez ainsi voire clairement quelles nouvelles vulnérabilités ont été identifiées ou comblées et, par conséquent, comment la protection de votre infrastructure évolue au fil du temps. Vous démasquez ainsi non seulement les vulnérabilités génériques, mais aussi celles qui sont spécifiquement contenues dans vos applications.

Dix ans d'expérience en matière de cybersécurité ont été mis à profit pour développer cette plateforme. Néanmoins, contrairement à d'autres scans de vulnérabilité, elle peut être utilisée sans expert en sécurité informatique et demande un budget limité.

1.3 Mesures – Réponse aux incidents

Même si vous vous préparez et formez vos collaboratrices et collaborateurs, un incident de sécurité peut survenir. En cas d'attaque, il est essentiel de réagir immédiatement et de manière ciblée. Nos spécialistes en sécurité vous aident à vous préparer au mieux. Lors d'un incident, vous pouvez en outre compter sur le soutien de notre équipe de réponse aux incidents. Nous veillons à ce qu'aucun temps précieux ne soit perdu et que les dommages causés à votre entreprise soient aussi limités que possible.

Équipe de réponse aux incidents – En cas d'urgence vous n'êtes pas seuls

Nous vous aidons à endiguer et à analyser les cyberincidents 24 heures sur 24 et 7 jours sur 7 et à rétablir les activités de votre entreprise. Votre équipe Redguard de réponse aux incidents couvre toutes les expertises nécessaires (technologie, exigences réglementaires, etc.) et est en contact permanent avec les autorités et les autres équipes de réponses aux incidents. Nous assurons un déroulement structuré de la prise en charge et gardons la tête froide.

Pour plus d'informations: https://www.redguard.ch/fr/consulting/cyber-security-incident/

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

- Site web de l'Office fédéral pour l'approvisionnement économique du pays :

  https://www.bwl.admin.ch/bwl/fr/home.html

- Factsheet norme minimale pour les TIC de Redguard

  https://www.redguard.ch/downloads/factsheet_ikt_minimalstandard_de.pdf

- Quick-Test de la norme minimale pour les TIC de Redguard

  DE: http://ikt.redguard.ch
  FR: http://ikt-fr.redguard.ch

- Site web de Redguard

  https://www.redguard.ch/fr/

Faites maintenant notre Cyber Security Quick Test en français : http://ikt-fr.redguard.ch

et déduisez-en des mesures!