FIDUCIAIRE | SUISSE
Union Suisse des Fiduciaires

La cybersécurité dans l'entreprise fiduciaire

I. Cybersécurité

Votre société pourrait devenir victime d'une cyberattaque. La cybersécurité concerne aujourd'hui toutes les entreprises qui tirent parti de la digitalisation. Il relève de la responsabilité de chaque entreprise de se procurer une protection individuelle, en adoptant des mesures organisationnelles et techniques afin de minimiser le potentiel et l'étendue du risque lié à une cyberattaque. Les mesures organisationnelles lui permettent d'améliorer la sécurité de son information, et la mise en place des mesures techniques contribue à augmenter la sécurité de son infrastructure TIC. Ces deux volets de mesures doivent se compléter pour garantir une protection adéquate de l'entreprise.

Parmi les cybermenaces potentielles figurent notamment des attaques affectant la disponibilité des systèmes (dénis de service distribués DDoS), les rançongiciels (« chevaux de Troie de verrouillage »), l'hameçonnage, les fuites de données, l'arnaque au président, le piratage d'une messagerie professionnelle (BEC), le piratage et l'arnaque à l'enregistrement de noms de domaine.

II. Test rapide de cybersécurité et guide pour les PME

La Confédération et plusieurs organisations[1] se sont associées pour développer un test rapide de cybersécurité destiné aux PME. Il permet aux entreprises d'évaluer leur niveau de protection contre les attaques venant du cyberespace et de vérifier si elles remplissent les standards minimum pour les PME.

En exécutant le test rapide, une PME peut évaluer si ses mesures techniques, organisationnelles et liées au personnel lui garantissent une protection adéquate contre les cyberrisques. Si l'analyse proposée n'est pas exhaustive et complète, le test permet néanmoins aux PME disposant de connaissances peu approfondies en informatique et en cybersécurité de faire le point sur leur situation, en posant les questions essentielles que toute entreprise se doit d'aborder. Le questionnaire peut être rempli aussi bien en ligne que hors ligne.

Vous trouverez le test rapide sur le site www.cybersecurity-check.ch, ainsi qu'un guide de la cybersécurité pour les PME (en langue anglaise) qui propose une assistance aux entreprises cherchant à obtenir une cybersécurité minimale et ainsi une protection accrue contre les cyberattaques les plus fréquentes. Le guide aborde les thèmes suivants : la sécurité dans les domaines de l'organisation et des processus, la sécurité grâce au facteur humain, grâce aux mesures techniques appropriées, la cybersécurité comme composante de la protection des données et la sécurité grâce à un environnement adéquat. Chaque thème est assorti de brèves explications sur son importance, sur les mesures pouvant être adoptées et sur la procédure à suivre.

III. Centre national pour la cybersécurité (NCSC)

Le Centre national pour la cybersécurité (National Cyber Security Centre NCSC) est le centre de compétences de la Confédération en matière de cybersécurité et le premier interlocuteur pour les milieux économiques, l'administration, les établissements d'enseignement et la population pour toute ques-

[1] digitalswitzerland, ISSS, satw, SNV, SQS et ASA/SVV

tion relative à la cybersécurité. Sa Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) comprend le nouveau guichet suisse unique qui réceptionne les notifications concernant les cyberincidents émanant de la population et des milieux économiques, les analyse et donne aux personnes ou aux services à l'origine du signalement une évaluation de l'incident concerné ainsi que des recommandations pour la suite de la procédure.

Le NCSC met à la disposition des entreprises des informations exhaustives sur la cybersécurité (https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-unternehmen.html).

Des informations et remarques sur les mesures préventives concernant les thèmes actuels suivants sont disponibles sur le site du NCSC :

- Tentatives des cyberattaques envers les entreprises : bon à savoir
- Collaborer avec des prestataires externes de services informatiques
- Home Office – sécuriser son accès à distance
- Norme minimale pour les TIC
- Mesures de protection pour les systèmes de gestion de contenu
- Mesures de protection pour les systèmes de contrôle industriels (SCI)
- Sécurité de l'Internet des objets
- Mesures contre les attaques DDoS
- Voyages à l'étranger
- Protégez vos comptes
- Sécurité de l'information : aide-mémoire pour PME
- Gestion sûre du courrier électronique
- Avez-vous les processus de paiement sous contrôle ?

Le NCSC offre également des informations et une assistance pour le cas où un cyberincident devait se produire :

- Rançongiciels – que faire ?
- Site web piraté – que faire ?
- Fuite de données – que faire ?
- Cyberattaque – que faire ? Aide-mémoire à l'intention des CISO
- Attaque DDoS – que faire ?

Un formulaire en ligne vous permet par ailleurs d'annoncer les cyberincidents ou les failles aisément à travers le web.

IV. Assurance contre le cyberrisque

L'importance des cyberrisques ne cesse de s'accroître dans l'activité quotidienne des entreprises et le niveau de risque augmente constamment. Le secteur des assurances a donc développé des polices d'assurance spéciales pour les cyberrisques qui permettent aux entreprises de s'assurer contre les composantes essentielles de leur risque. En général, les assurances cyberrisques se composent de plusieurs modules, mais la protection offerte par les modules de différents assureurs peut différer. Nous vous recommandons donc de procéder à une comparaison de plusieurs solutions d'assurances en vous basant sur une analyse du risque ou du besoin d'assurance spécifique à votre entreprise et aussi de comparer celles-ci avec les polices d'assurance conclues pour éviter d'avoir des lacunes de couverture ou des assurances doubles.

V. Offre et soutien de la part de FIDUCIAIRE|SUISSE

Afin de tenir compte de la thématique de la cybersécurité dans l'entreprise fiduciaire, FIDUCIAIRE|SUISSE créera, en début d'été 2022, une centrale de contact chargée de traiter toute question y relative. En plus d'informations générales sur la sécurité, la centrale publiera notamment des articles destinés à sensibiliser le personnel, les possibilités ouvertes aux entreprises pour tester leur cybersécurité, ainsi qu'une offre d'assistance pour obtenir une protection optimisée.

Nous vous tiendrons au courant. Pour être toujours au fait de l'actualité en matière de cybersécurité, abonnez-vous également aux informations de l'Institut Fiduciaire 4.0 dans les réseaux sociaux.

Institut fiduciaire et droit et Institut fiduciaire 4.0 / février 2022