enisa

AGENCE DE L'UNION EUROPÉENNE
POUR LA CYBERSÉCURITÉ

Guide de la cybersécurité pour les PME

12 MESURES

POUR SÉCURISER VOTRE ENTREPRISE

La crise liée à la COVID-19 a mis en évidence l'importance de l'internet et des ordinateurs en général pour les PME. Pour continuer à prospérer pendant la pandémie, de nombreuses PME ont dû prendre des mesures de continuité des activités telles que le recours aux services en nuage, l'amélioration de leur service internet, la mise à jour de leurs sites web et l'instauration du travail à distance.

Cette brochure propose aux PME des mesures pratiques de haut niveau visant à mieux sécuriser leurs systèmes et leurs activités. Elle vient compléter le rapport plus détaillé de l'ENISA intitulé **«Cybersecurity for SMES – Challenges and Recommendations»**.

1 DÉVELOPPER UNE CULTURE DE LA CYBERSÉCURITÉ

RESPONSABILITÉ DE GESTION

Le succès durable de toute PME passe par la mise en place d'une cybersécurité de qualité. La responsabilité de cette fonction essentielle devrait être confiée à une personne, au sein de l'organisation, chargée de veiller à l'affectation de ressources appropriées: le temps du personnel, l'achat de logiciels, de services et de matériel de cybersécurité, la formation du personnel et l'élaboration d'une politique efficace en la matière.

ADHÉSION DU PERSONNEL

La direction devrait favoriser l'adhésion du personnel à travers une communication efficace sur la cybersécurité, et en soutenant ouvertement les initiatives dans ce domaine, en dispensant des formations appropriées à l'intention du personnel et en énonçant des règles claires et spécifiques dans le cadre de la politique de cybersécurité.

POLITIQUE DE CYBERSÉCURITÉ

Des règles claires et spécifiques devraient être énoncées dans la politique de cybersécurité à l'intention des employés, concernant la conduite à tenir lorsqu'ils utilisent l'environnement, les équipements et les services TIC de l'entreprise. Cette politique devrait aussi souligner les conséquences auxquelles le personnel s'exposerait en cas de non respect de ses dispositions. La politique doit être régulièrement révisée et mise à jour.

AUDITS DE CYBERSÉCURITÉ

Des audits réguliers devraient être réalisés par des personnes disposant des connaissances, des compétences et de l'expérience appropriées. Les auditeurs devraient être indépendants – des contractants externes ou internes – et ne pas avoir de liens avec les opérations informatiques quotidiennes.

PROTECTION DES DONNÉES

En vertu du règlement général de l'UE sur la protection des données,[1] toute PME qui traite ou stocke des données à caractère personnel concernant des personnes résidant dans l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont en place pour protéger ces données. Cela implique notamment de s'assurer que tous les tiers travaillant pour le compte de la PME ont mis en place des mesures de sécurité appropriées.

1 Règlement général sur la protection des données (RGPD) https://ec.europa.eu/info/law/law-topic/data-protection_fr

2

DISPENSER UNE FORMATION APPROPRIÉE

Organisez régulièrement des formations de sensibilisation à la cybersécurité pour tous les employés en vue de leur donner les moyens de reconnaître et de traiter les différentes cybermenaces. Ces formations devraient être adaptées et cibler les situations réelles des PME.

Proposez une formation en cybersécurité spécialisée aux personnes responsables de gérer la cybersécurité au sein de l'entreprise pour les doter des compétences et aptitudes nécessaires à l'exercice de leurs fonctions.

3

GÉRER EFFICACEMENT LES TIERS

Veillez à ce que tous les fournisseurs, notamment ceux ayant accès à des données et/ou des systèmes sensibles, fassent l'objet d'une gestion active et respectent les niveaux de sécurité convenus. Des accords contractuels devraient être établis pour régir les modalités de mise en œuvre de ces exigences de sécurité par les fournisseurs.

4

ÉLABORER UN PLAN DE RÉACTION AUX INCIDENTS

Préparez un plan formel de réaction aux incidents définissant clairement des lignes directrices, ainsi que les rôles et responsabilités documentés, pour garantir que tous les incidents de sécurité fassent l'objet d'une réaction rapide, professionnelle et appropriée. Pour répondre rapidement aux cybermenaces, recherchez des outils susceptibles de surveiller et de générer des alertes en cas d'activité suspecte ou de violation de la sécurité.

5 SÉCURISER L'ACCÈS AUX SYSTÈMES

Encouragez tous les membres du personnel à utiliser une phrase secrète composée d'au moins trois mots courants choisis au hasard et combinés pour former une expression facile à mémoriser et sûre. Si vous optez pour un mot de passe classique:

- choisissez-le relativement long, avec des caractères minuscules et majuscules, et éventuellement des chiffres et des caractères spéciaux;
- évitez les évidences, comme «mot de passe», les séquences de lettres ou de chiffres telles «abc» ou «123»;
- évitez d'utiliser des informations personnelles qui peuvent être trouvées en ligne.

Que vous utilisiez des phrases ou des mots de passe:

- ne les réutilisez pas ailleurs;
- ne les communiquez pas à vos collègues;
- activez l'authentification multifacteurs;
- utilisez un gestionnaire de mots de passe dédié.

6 SÉCURISER LES APPAREILS

La sécurité des appareils utilisés par le personnel, (ordinateurs de bureau, portables, tablettes ou smartphones) est un aspect essentiel d'un programme de cybersécurité.

CORRECTIFS ET MISES À JOUR DES LOGICIELS

L'idéal consiste à utiliser une plateforme centralisée pour gérer les correctifs. Il est vivement recommandé aux PME de:

- mettre à jour régulièrement tous leurs logiciels;
- activer les mises à jour automatiques dans la mesure du possible;
- recenser les logiciels et le matériel nécessitant des mises à jour manuelles;
- prendre en compte les appareils mobiles et les appareils IDO.

ANTI-VIRUS

Une solution antivirus centralisée devrait être utilisée sur tous les types d'appareils, et mise à jour pour assurer son efficacité continue. N'installez pas de logiciels piratés, car ils pourraient contenir des programmes malveillants.

PROTECTION DU COURRIER ÉLECTRONIQUE ET DU WEB

Recourez à des solutions permettant de bloquer les pourriels, les courriels comportant des liens vers des sites internet malveillants, les courriels contenant des pièces jointes malveillantes telles que des virus, et les courriels d'hameçonnage.

CRYPTAGE

Protégez les données en les cryptant. Les PME devraient veiller à ce que les données stockées dans les appareils mobiles (portables, smartphones et tablettes) soient cryptées. Pour les données transférées sur des réseaux publics tels que les réseaux WiFi des hôtels ou des aéroports, assurez-vous que les données sont cryptées, en utilisant un réseau privé virtuel (RPV) ou en accédant aux sites web via des connexions sécurisées à l'aide du protocole SSL/TLS. Veillez à ce que vos propres sites web utilisent une technologie de cryptage appropriée pour protéger les données des clients lorsqu'elles transitent sur internet.

7 SÉCURISER VOTRE RÉSEAU

GESTION DES APPAREILS MOBILES

Pour faciliter le travail à distance, de nombreuses PME autorisent leurs employés à utiliser leurs propres ordinateurs portables, tablettes et/ou smartphones. Cette pratique engendre des problèmes de sécurité liés aux données professionnelles sensibles conservées sur ces appareils. Pour prévenir d'éventuels problèmes, une PME peut recourir à une solution de gestion des appareils mobiles (GAM) qui lui permettra de:

- contrôler les appareils autorisés à accéder à ses systèmes et services;
- s'assurer que l'appareil est équipé d'un logiciel antivirus à jour;
- vérifier si l'appareil est crypté;
- confirmer que l'appareil dispose des correctifs logiciels les plus récents;
- veiller à ce que l'appareil soit protégé par un code PIN et/ou un mot de passe;
- effacer à distance toutes les données professionnelles si le propriétaire de l'appareil déclare sa perte ou son vol, ou en cas de cessation du contrat de travail avec la PME.

PARE-FEU

Les pare-feu gèrent le trafic entrant et sortant d'un réseau et constituent un outil essentiel pour la protection des systèmes informatiques des PME. Ils devraient être déployés pour protéger tous les systèmes critiques, et en particulier pour protéger le réseau des PME contre les menaces sur internet.

SOLUTIONS D'ACCÈS À DISTANCE

Les PME devraient régulièrement passer en revue tous les outils d'accès à distance pour vérifier qu'ils sont sécurisés, et en particulier:

- vérifier que tous les logiciels d'accès à distance ont les derniers correctifs et mises à jour;
- limiter l'accès à distance depuis des adresses IP ou des lieux géographiques suspects;
- limiter l'accès à distance des employés aux seuls systèmes et ordinateurs dont ils ont besoin pour leur travail;
- imposer des mots de passe robustes pour l'accès à distance et, dans la mesure du possible, activer l'authentification multifacteurs;
- prévoir l'activation d'un dispositif de surveillance et d'alerte pour signaler toute attaque ou activité inhabituelle suspecte.

8 AMÉLIORER LA SÉCURITÉ PHYSIQUE

Il conviendrait de mettre en place des contrôles physiques appropriés pour tous les supports contenant des informations essentielles. Un ordinateur portable ou un smartphone d'entreprise, par exemple, ne devrait pas être laissé sans surveillance sur le siège arrière d'une voiture. Tout utilisateur devrait verrouiller son ordinateur dès lors qu'il s'en éloigne, ou activer la fonction de verrouillage automatique. Il ne faut pas non plus laisser les documents sensibles imprimés sans surveillance; lorsqu'ils ne sont pas utilisés, ils devraient être rangés en lieu sûr.

9 SÉCURISER LES SAUVEGARDES

Il est recommandé de réaliser des sauvegardes, car elles offrent un moyen efficace de récupérer des données essentielles en cas d'attaque par un rançongiciel ou autre catastrophe. Les règles de sauvegarde suivantes devraient s'appliquer:

- la sauvegarde est régulière et automatisée dans la mesure du possible;
- la sauvegarde est conservée séparément de l'environnement de production de la PME;
- les sauvegardes sont cryptées, tout particulièrement si elles doivent être déplacées d'un endroit à l'autre;
- la capacité de restauration régulière des données à partir des sauvegardes est testée. Idéalement, il faudrait effectuer régulièrement un test de restauration d'une sauvegarde complète.

10 OPTER POUR l'INFORMATIQUE EN NUAGE

Si elles offrent de nombreux avantages, les solutions en nuage présentent aussi certains risques particuliers, que les PME devraient prendre en compte avant de s'engager auprès d'un fournisseur de services en nuage. L'ENISA a publié un document intitulé «Cloud Security Guide for SMEs»[2] auquel les PME devraient se référer lors de la migration vers le nuage.

Lors de la sélection de leur fournisseur de services, les PME devraient s'assurer qu'il ne viole aucune loi ou réglementation en stockant des données, notamment des données à caractère personnel, en dehors de l'UE/EEE. Par exemple, en vertu du RGPD de l'UE, les données à caractère personnel des personnes résidant dans l'UE/EEE ne doivent pas être conservées ou transmises en dehors de l'UE/EEE, excepté dans des conditions très spécifiques.

2 https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

11 SÉCURISER LES SITES EN LIGNE

Les PME doivent s'assurer que leurs sites web en ligne sont configurés et entretenus de manière sécurisée et que toutes les données à caractère personnel ou les informations financières, telles que les données des cartes de crédit, sont correctement protégées. À cette fin, il convient d'effectuer régulièrement des tests de sécurité sur les sites web afin d'identifier tout point faible potentiel en matière de sécurité et de procéder à des examens réguliers pour s'assurer que le site est entretenu et mis à jour correctement.

12 RECHERCHER ET PARTAGER DES INFORMATIONS

Le partage d'informations relatives à la cybercriminalité est un moyen efficace de lutter contre cette forme de criminalité. Il joue un rôle essentiel pour permettre aux PME de mieux comprendre les risques auxquels elles sont confrontées. Les entreprises qui entendent des témoignages de leurs homologues concernant des problèmes de cybersécurité et les moyens mis en œuvre pour y remédier, seront plus susceptibles de prendre des mesures pour sécuriser leurs systèmes que si elles sont informées par le biais de rapports sectoriels ou d'enquêtes sur la cybersécurité.

AGENCE DE L'UNION EUROPÉENNE
POUR LA CYBERSÉCURITÉ

À PROPOS DE L'ENISA

L'Agence européenne pour la cybersécurité (ENISA) est l'agence de l'Union européenne qui vise à garantir un niveau élevé commun de cybersécurité dans toute l'Europe. Créée en 2004 et renforcée par le règlement de l'Union européenne sur la cybersécurité, l'ENISA contribue à la politique de l'Union en matière de cybersécurité, améliore la fiabilité des produits, services et processus TIC à l'aide de schémas de certification de cybersécurité, coopère avec les États membres et les organes de l'Union, et aide l'Europe à se préparer aux défis informatiques de demain. En partageant les connaissances, en renforçant les capacités et en organisant des initiatives de sensibilisation, l'Agence œuvre de concert avec ses principales parties prenantes pour renforcer la confiance dans l'économie connectée, améliorer la résilience des infrastructures de l'Union et, au bout du compte, maintenir la sécurité numérique de la société européenne et de ses citoyens. Pour plus d'informations, consultez: www.enisa.europa.eu.

ENISA
Agence de l'Union européenne pour la cybersécurité

Bureau d'Athènes
Ethnikis Antistaseos 72 &
Agamemnonos 14,
Chalandri 15231, Attiki, Grèce

Bureau d'Héraklion
95 Nikolaou Plastira
700 13 Vassilika Vouton,
Héraklion, Grèce

enisa.europa.eu