FEDIL

Publication - 22/05/2020

CYBERSECURITY CHECKLIST

Mesdames et messieurs,

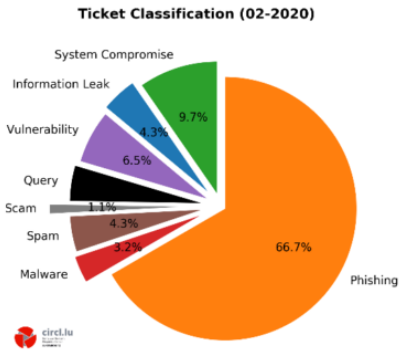
Chers membres,

La FEDIL, en collaboration avec SECURITYMADEIN.LU, souhaite attirer votre attention sur certains éléments de cybersécurité à prendre en considération afin de limiter les risques et de prévenir dans la mesure du possible les cyberattaques qui se multiplient et se diversifient.

Il est en permanence important de garder un œil attentif sur la cybersécurité au sein de son entreprise et de s'assurer de la mise en place de mesures adéquates et ce, plus que jamais dans le contexte de la crise du coronavirus, de par le recours massif au télétravail qui ouvre des opportunités pour les attaquants. Le télétravail favorise l'utilisation des e-mails pour la communication, créant ainsi des conditions parfaites pour les stratagèmes de fraude par e-mail.

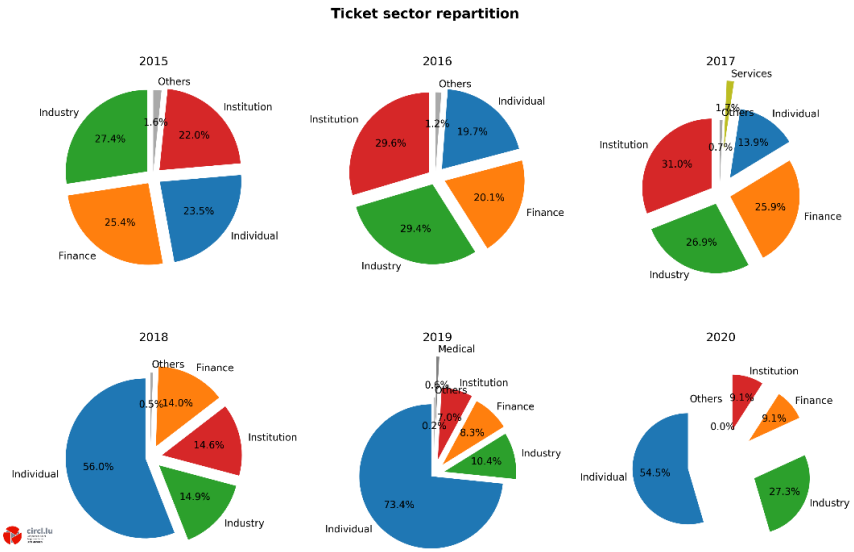
En effet, même si le nombre d'attaques n'augmente pas de manière significative, un certain type connait une recrudescence à savoir le phishing. Les chiffres du CIRCL de février dernier montrent l'importance de telles attaques avec 66,7 % (voir graphique ci-dessous). C'est là que le bât blesse dans la mesure où ce type d'attaque exploite le facteur humain et s'adresse directement aux utilisateurs qui ne sont souvent pas suffisamment préparés à identifier un email frauduleux. La motivation de ces attaques est prioritairement financière. La finalité est de monnayer les informations obtenues contre une rançon, les fameux «ransomware».

Les derniers exemples locaux en date ont ciblé les entreprises Cactus et Tarkett, mentionnées dans la presse. Dans le cas de Cactus, le groupe a été la cible du ransomware REvil. Les données volées par les hackers ont été publiées sur internet afin de forcer le groupe à payer la rançon demandée.



Il est dès lors primordial de sensibiliser les collaborateurs de l'entreprise aux risques qui peuvent être encourus suite à une mauvaise utilisation des dispositifs, à un mauvais comportement ainsi qu'aux conséquences d'une cyberattaque.

Par ailleurs, comme le montre le graphique ci-dessous, tous les secteurs d'activité dépendants des infrastructures informatiques, indépendamment de la taille de l'entreprise, sont visés.



En conséquence, la FEDIL vous rappelle ci-dessous les conseils pratiques proposés par SECURITYMADEIN.LU

DISPOSITIFS

- Faire particulièrement attention à ce que les appareils tels que les clés USB, les téléphones, les ordinateurs portables ou les tablettes ne soient pas perdus ou égarés.
- Utiliser de préférence l'ordinateur professionnel. Si ce n'est pas possible, vérifier les mises à jour avant d'utiliser l'ordinateur privé. Mettre en place des comptes séparés pour les membres de la famille.
- S'assurer que chaque appareil dispose des mises à jour nécessaires, telles que les mises à jour du système d'exploitation (comme iOS ou Android) et les mises à jour logicielles / antivirus.
- S'assurer que l'ordinateur, ordinateur portable ou appareil, soit utilisé dans un endroit sûr, par exemple où il peut être vu, et minimiser qui

d'autre peut voir l'écran (en particulier si la personne travaille avec des données personnelles sensibles).
- Verrouiller l'appareil s'il doit être laissé sans surveillance pour une raison quelconque.
- S'assurer que les appareils soient éteints, verrouillés ou stockés avec soin lorsqu'ils ne sont pas utilisés.
- Obturer la caméra lorsqu'elle n'est pas utilisée.
- Utiliser des contrôles d'accès efficaces (tels que l'authentification multi facteur et des mots de passe forts) et, le cas échéant, le cryptage pour restreindre l'accès à l'appareil et pour réduire le risque si un appareil est volé ou égaré.
- Lorsqu'un appareil est perdu ou volé, prendre des mesures immédiates pour assurer un effacement de la mémoire à distance, si possible.

E-MAILS

- Utilisez des comptes de messagerie professionnels plutôt que des comptes personnels pour les e-mails liés au travail impliquant des données personnelles. Si e-mail personnel est utilisé, s'assurer que le contenu et les pièces jointes soient cryptés et éviter d'utiliser des données personnelles ou confidentielles dans les lignes d'objet.
- Avant d'envoyer un e-mail, s'assurer de l'envoyer au bon destinataire, en particulier pour les e-mails impliquant de grandes quantités de données personnelles ou des données personnelles sensibles.
- Si possible, préférer envoyer des e-mails chiffrés à chaque fois.

ACCÈS AU CLOUD ET AU RÉSEAU

- Configurer les appareils au préalable par la mise en place d'outils tels que des pare-feux (en anglais «firewall») ainsi que des règles d'hygiène informatique.
- Utiliser un réseau privé virtuel (VPN) pour assurer une connexion de manière directe et sécurisée avec le réseau interne de la société et permettre de protéger le transfert de données de tout acte malveillant.
- Ne se connecter à aucun réseau public Wi-Fi, inconnu ou non contrôlé. Ces réseaux sont souvent utilisés par des acteurs malveillants comme des vecteurs d'attaque privilégiés afin de cibler les entreprises au travers de leurs collaborateurs.
    - Connectez-vous aux réseaux 3G ou 4G si vous n'avez pas accès à une connexion Wi-Fi sécurisée
- Dans la mesure du possible, utiliser uniquement les réseaux ou services de confiance de l'organisation et respecter toutes les règles et procédures organisationnelles concernant l'accès au cloud ou au réseau, la connexion et le partage de données.
- Si vous travaillez sans accès au cloud ou au réseau, s'assurer que toutes les données stockées localement sont correctement sauvegardées en toute sécurité.
- Les logiciels d'accès à distance (comme TeamViewer) doivent être utilisés très soigneusement et uniquement par des employés autorisés. Il doit toujours être mis à jour et utilisé uniquement en cas de nécessité absolue.
- Vérifier la fiabilité des plateformes de vidéoconférence. Notamment, où sont stockés les fichiers lorsque qu'ils sont transférés. Il en va de même pour les plateformes de transfert de fichiers.

VISIO-CONFÉRENCE

L'utilisation de la visio-conférence comporte également des risques. Il existe principalement 3 types de risques :

- Le principal risque à couvrir est une fuite de données par une écoute passive et non autorisée de discussions confidentielles.
- Les risques liés à une atteinte à la vie privée suite à une mauvaise utilisation, paramétrage ou failles logiciels permettant par exemple : la prise de contrôle de la caméra de l'organisateur à son insu, l'enregistrement de l'appel ou encore l'envoi de données des comptes utilisateurs à des tiers sans autorisation…
- Les documents, présentations, notes et autres chat messages échangés (en plus de la voix) qui peuvent contenir des informations sensibles et qui peuvent se retrouver sur des serveurs non maîtrisés.

Nous vous invitons à suivre les recommandations de SECURITYMADEIN.LU afin de limiter les risques au lien suivant: VISIOCONFÉRENCE ET CYBERSÉCURITÉ: COMMENT LIMITER LES RISQUES?

Par ailleurs, il est à noter que les attaquants essaient de tirer profit de la crise du coronavirus en capitalisant sur la peur et l'incertitude générée par le COVID-19. Ci-dessous une liste non-exhaustive de cas auxquels vous pouvez être confrontés.

1. Sites web dédiés au coronavirus: certains attaquants conçoivent des sites web relatifs au coronavirus afin de vous inviter à télécharger une application pour vous tenir informés de la situation. Mais c'est un piège!
2. Mesures de sécurité contre le coronavirus: vous êtes invité à télécharger un pdf contenant des conseils pour vous protéger contre le virus. Mais le fichier pdf contient du code malveillant…
3. Faux antivirus contre le coronavirus: si vous l'installez, il crée des portes dérobées sur votre ordinateur.
4. Des imposteurs se faisant passer pour la Croix-Rouge vendent des tests COVID-19 à domicile.
5. Un faux message de l'OMS (Organisation Mondiale de la Santé) installe un logiciel espion sur votre ordinateur.
6. Chantage au travers d'e-mails qui menacent de vous infecter avec le coronavirus.
7. Canulars téléphoniques du CDC demandant aux gens de réserver les vaccins contre le COVID-19.
8. Arnaques promettant des chèques de 1000 $ comme aide économique en cas de pandémie.
9. Diverses escroqueries « Rester en sécurité contre le coronavirus ».
10. Codes de réduction COVID-19 pour vendre des logiciels malveillants et des contrefaçons.
11. Les plateformes de communication instantanée sont des cibles privilégiées pour les cybercriminels.
12. Dans ce contexte, le nombre de fausses actualités, «fake news», est également en augmentation.

Enfin, nous souhaitons souligner l'émergence d'un autre phénomène qui permet d'accéder au réseau de l'entreprise par le collaborateur mais dont il est difficile de connaitre l'impact. Il s'agit de l'utilisation de la sphère privée et de l'envoi d'e-mails d'extorsion avec comme sujet «Je connais ton mot de passe». L'attaquant prétend détenir des informations compromettantes sur la personne et demande le paiement d'une rançon. Nous vous recommandons fortement de sensibiliser vos collaborateurs à ce mode d'attaque et de les inviter à suivre les recommandations de SECURITYMADEIN.LU: SEXTORTION SCAM E-MAILS: « I KNOW YOUR PASSWORD »

Crise du coronavirus ou non, il est capital d'agir avec la plus grande prudence lors de la consultation des e-mails et des sites internet et en cas de doute, il est fortement recommandé de consulter et d'alerter le département informatique et les spécialistes de la cybersécurité.