Partages d'expériences liées à la cybersécurité en temps de COVID-19

A.ROCHAIS, 25 mai 2020, Livre Blanc NETIA

Table des matières

Introduction

Par ce livre blanc axé sur les risques cyber émergeants à prendre en compte pendant la crise du COVID-19, NETIA souhaite vous faire partager son expérience, ses initiatives et ses connaissances en la matière.

Les menaces émergentes liées à la crise COVID-19

Les agents de menaces

La crise du COVID-19 a bouleversé les habitudes de travail de bon nombre de sociétés en les forçant à basculer rapidement en télétravail.

Certaines entreprises avaient déjà intégré une part de télétravail à leurs habitudes mais très rarement pour la totalité de leurs collaborateur·ices en simultané.

Cette avancée à marche forcée occasionne des vulnérabilités non maitrisées en termes de cyber sécurité.

Les agents de menace (c'est-à-dire des personnes ou des choses, qui agissent, ou ont la volonté et le pouvoir d'agir, de provoquer, transporter, transmettre ou soutenir une menace) ont perçu cette fébrilité cyber de la part des entreprises et redoublent donc d'activité sur cette période.

Les groupes sponsorisés par les états

De nombreux groupes de hackers sponsorisés par des états ont d'ores et déjà utilisé le thème du COVID-19 pour atteindre les cibles visées (étatiques ou non) en utilisant des attaques assez complexes :

- Vicious Panda (groupe suspecté d'être sponsorisé par l'état Chinois) a par exemple compromis des nombreuses cibles du secteur public de Mongolie à travers un document texte de format .rtf envoyé via des campagnes de spear phishing (phishing ciblé) en provenance apparente du ministère des affaires étrangères de Mongolie.
- Le groupe Hades (soupçonné d'être sponsorisé par la Russie) a utilisé la même porte d'entrée pour déployer des chevaux de Troie (via un envoi de mail ayant l'apparence de provenir du centre de santé publique du ministère de la santé ukrainien) pour attaquer des cibles chinoises.

Les exemples sont nombreux mais les attaques provenant de groupes sponsorisés par les états restent minoritaires mais non négligeables dans le domaine des médias.

Ces attaques bien que minoritaires déploient d'importants moyens pour arriver à leur but.

Les groupes de cybercriminels

La majorité des attaques recensées provient de groupes de cybercriminel·les (entendez par là des groupes motivés principalement par l'appât du gain).

Selon la société Proofpoint (USA), 80% des menaces de la période actuelle surfent sur la thématique du COVID-19 pour atteindre leurs cibles.

Un niveau de risque élevé dans le domaine des médias

Les médias (audiovisuels, télévisuels, numériques) sont une cible de choix pour les attaquants des groupes étatiques (cyberguerre) ou non étatiques (hacktivistes, cybercriminel·les). Avoir la main mise sur l'information est effectivement une cible stratégique pour toute personne souhaitant déstabiliser un état ou un média indépendant, ce qui a poussé nombre d'états à protéger ces canaux de communication.

Des recommandations précises sont faites à cet effet dans le cadre de l'EBU R143.

Les exemples ayant faits suite à l'attaque de TV5 Monde (perpétuée par un groupe lié à l'organisation terroriste « Etat Islamique ») sont nombreux en 2019 : Groupe M6, Sveriges Television (Suède), Cadena Ser Radio (Espagne), N1 TV (Serbie)…

Les menaces liées au télétravail

Les principales menaces liées au télétravail sont les suivantes :

Menaces sur les actifs organisationnels

Entendez par là la destruction, le vol, la diffusion, le détournement ou le blocage d'actifs critiques pour les entreprises/organisations.

Ces actifs critiques sont les actifs vitaux pour l'activité de l'entreprise (système de production, codes sources, site web, image de marque…)

Les actifs organisationnels comprennent également tous les actifs critiques pour des parties prenantes externes à une entreprise.

Menaces sur les actifs personnels

Entendez par là le vol, la revente, la diffusion, l'utilisation frauduleuse ou l'usurpation d'actifs personnels.

Les actifs personnels peuvent être l'identité des personnel·les, ou tout autre chose pouvant être liée à l'identité d'une personne (compte bancaire, sécurité sociale…).

Chaque entreprise européenne est tenue de protéger ces actifs dans le cadre du RGPD.

Les principaux types d'attaques

Phishing/Spear Phishing

Le phishing est un procédé qui permet d'acquérir de l'information privée ou de déployer un agent malveillant (comme un ransomware) en se faisant passer pour une entité digne de confiance.

Ceci se passe le plus généralement par l'envoi de mail.

Le spear phishing est en quelque sorte un phishing très ciblé faisant suite à un travail d'ingénierie sociale (prise d'informations précises sur les cibles visant à les tromper plus facilement).

Ransomware (ou rançongiciel)

Les Ransomware sont des logiciels malveillants prenant en otage les données personnelles ou organisationnelles, pouvant bloquer totalement un système de production.

Pour pouvoir espérer récupérer l'accès aux systèmes ou données cryptées, l'entreprise doit payer une rançon aux attaquants. Les nouvelles technologies de Ransomware intègrent également la fuite de données (les données en plus d'être cryptées sont volées et les attaquants menacent de diffuser les informations publiquement en cas de non-paiement de la rançon).

Déni de service

Ceci se caractérise par les tentatives des attaquants d'empêcher les utilisateurs légitimes d'un service d'utiliser ce service (système de production, site web…)

Ce genre d'attaque peut prendre plusieurs formes. Différents types de protections peuvent être utilisé que ce soit au niveau réseau (Firewall, IDS) ou au niveau applicatif (WAF). Des produits gratuits sont d'ailleurs utilisables sur site ou sur le cloud tel que le reverse proxy KEMP.

Des initiatives gratuites à destination des sites d'actualité sont mises en place tel que Project Shield.

Les vulnérabilités liées à la généralisation du travail distant

Vulnérabilités sur les outils de travail à distance

Les systèmes utilisés pour le travail à distance (Citrix, Zoom, Fortigate VPN…) ont présenté dernièrement des vulnérabilités utilisées pour le déploiement de Ransomware au sein de systèmes de production ou pour commettre un vol de données. L'exemple du système de visioconférence Zoom est très parlant (vol de 530 000 comptes utilisateurs, ainsi que des liens et identifiants d'accès aux réunions).

L'augmentation des attaques par brute force sur les accès via RDP (Remote Desktop Protocol) depuis le début du confinement, remontée par Symantec est un autre exemple parlant à prendre en compte.

Les vulnérabilités structurelles

- Multiplication des accès externes au réseau d'entreprise ou aux outils de production
- Les vulnérabilités entrainées par l'absence de mise à jour des systèmes et des applicatifs
- Les utilisateur·ices, à leur domicile, faute d'outils adaptés et confrontés à la surcharge de leur service informatique sont souvent contraints d'utiliser des services non adaptés aux contraintes de sécurité de l'entreprise
- La présence de vulnérabilités au sein des logiciels utilisés pour la production
- Utilisation de réseaux personnels non sécurisés

L'humain

Les employé·es représentent des risques importants pour l'entreprise et pour leurs propres données personnelles. Les risques proviennent aussi bien de leur utilisation d'outils informatiques que par les tentatives de tromperie qui peuvent les cibler (phishing) et des conséquences qu'elles peuvent avoir en l'absence de sensibilisation.

NETIA@Home, partages d'expériences sur les actions mises en place par NETIA

Initiatives NETIA auprès des clients pendant la crise du COVID-19

Afin d'accompagner au mieux ses clients dans cette période de changement, leur permettre de maintenir la production tout en limitant les risques introduit par ces nouveaux usages, NETIA a lancé l'initiative NETIA@Home.

Kit@Home

Il s'agit de solutions construites autour de cas d'usages simples qui permettent aux utilisateur·ices de répliquer leurs workflows dans les conditions de travail à distance. Ces développements sont testés par nos radios partenaires et leurs utilisateur·ices afin de conjuguer l'expérience client à une solution sécurisée adaptée à l'environnement de chaque radio.

Les outils mis à disposition permettent aux utilisateur·ices de travailler de manière autonome depuis chez eux et d'intégrer de manière sécurisée ces éléments au système de production central du client via FTPS.

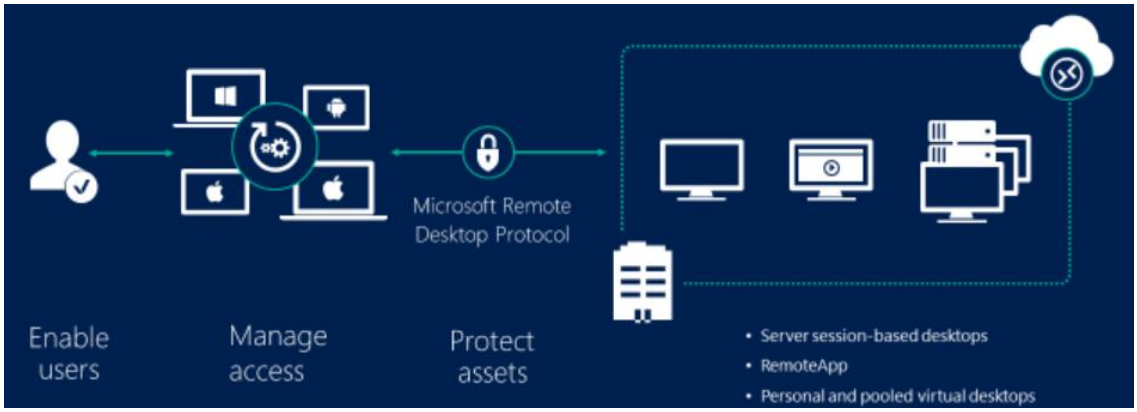
Un Browser web livré sous forme de web service aux clients permet aux utilisateur·ices de se connecter de manière sécurisée aux bases de données situées dans leurs locaux. Ce browser web est accessible en HTTPS, intègre des moyens d'authentification modernes conformes aux meilleures pratiques de l'OWASP, et NETIA avant livraison effectue des tests statiques et dynamiques de sécurité des applications.

Enterprise@Home

Les solutions pour accéder à RadioAssist dans son intégralité, comme au bureau mais à distance sont regroupées dans Enterprise@Home. Il s'agit ici d'accompagner les DTSI pour intégrer les collaborateur·ices à distance dans la production et la réalisation de la radio.

Les meilleures pratiques identifiées suivantes sont abordées :

- Mise en place de machines virtuelles
    - VMware, Hyper-V
- Utilisation du RDP
    - Accès aux outils de production via Microsoft RemoteApp sécurisé et durcissement des systèmes d'exploitation.



- Utilisation du cloud
    - Microsoft Azure, VMware Horizon…
- Utilisation des tunnels sécurisés (VPN) pour accès à certaines parties des outils de production

Pour accompagner les démarches de ses clients tout en assurant la sécurité de leur organisation, NETIA est disponible pour recommander des durcissements lors de l'ouverture des web services sur le réseau internet, lors d'une implémentation d'accès à distance ou sur tout autre sujet pouvant mettre en péril la cybersécurité de leur organisation.

Réduction des risques liés à la généralisation du télétravail chez NETIA

Afin de sécuriser au mieux les salariés de la société et les intérêts de ses clients, NETIA a mis en place les actions suivantes parmi d'autres :

- Campagnes de phishing interne destinées à la sensibilisation du personnel (intégrant la falsification d'identité des expéditeurs, les pièces jointes malveillantes et les liens vers site malveillants).
- Mise en place de contrôles de sécurité et monitoring sur les accès distants.
- Mise en place de l'authentification multifacteurs sur les comptes sensibles avant généralisation
- Processus actif et contrôlé de mise à jour des OS et des logiciels utilisés.

- Analyse des vulnérabilités des postes utilisateur·ices et des serveurs.
- Mise en place de protections basées sur l'intelligence artificielle et l'analyse comportementale.

En conclusion; dans le cyberespace, le déni de risque n'est pas une option, NETIA vous invite donc à prendre en considération les menaces et risques détaillées dans ce document et à nous contacter pour vous accompagner sur :

- Les contre-mesures de protection
- Les moyens de contrôle adaptés
- Les outils mis en place par NETIA pour faciliter le travail à distance