Cybersécurité
2021

Par POST Cyberforce

CYBERFORCE.lu

POST LUXEMBOURG

SOMMAIRE

GRAND ENTRETIEN

Jean-Marie Bourbon (Head of Offensive Security), **Régis Jeandin** (Head of CyberDefense), **Alain Hirtzig** (Head of Telecom Security), **Olivier Antoine** (Head of Information Security Management)

« L'enjeu ? Être préparé à faire face à tout incident »

Quels enseignements les experts de POST Cyberforce tirent-ils de l'année 2021 ?

« *Au cœur de l'année 2021, l'événement le plus marquant a certainement été le signalement et l'exploitation par des acteurs malintentionnés de la vulnérabilité log4j* », commente Jean-Marie Bourbon, Head of CyberForce Offensive Security au sein de POST Luxembourg. Cette vulnérabilité ressemble à bien des égards à la cyberattaque contre *SolarWinds*, qui constituait une menace à grande échelle à laquelle les acteurs du monde entier ont dû faire face un an plus tôt.

Log4j est une bibliothèque logicielle utilitaire open source programmée en langage Java. Celui-ci étant extrêmement répandu et présent dans de nombreux logiciels, la vulnérabilité associée à ces éléments constituait une menace considérable pour bon nombre d'acteurs. « *Le schéma associé à ce type de menace est souvent similaire. Des acteurs malveillants exploitent le fruit du travail d'un chercheur en sécurité informatique, qui a mis à jour une vulnérabilité,* explique Olivier Antoine, Head of Information Security Management au sein de POST Luxembourg. *Le plus souvent, c'est un vendredi, dans une période proche de la fin de la semaine, quand tout le monde a la tête ailleurs, que ces vulnérabilités sont signalées et exploitées.* »

Vulnérabilité Zero Day : s'y préparer

Pour les équipes de POST, opérateur ayant une empreinte considérable sur le marché, l'émergence de ces nouvelles vulnérabilités exige de réagir rapidement. On parle de vulnérabilité « **Zero Day** », autrement dit de l'exploitation d'une faille jusqu'alors en dehors de tout radar, à laquelle il faut remédier avant toute compromission. « *L'enjeu, c'est d'être en capacité de réagir le plus rapidement possible à ce type d'attaque,* relève Alain Hirtzig, Head of Telecom Security au sein de POST Luxembourg. *Il faut minimiser le temps entre le moment où la vulnérabilité est mise à jour et l'application d'un correctif. Mais encore faut-il savoir si, oui ou non, l'entreprise y est exposée, si les systèmes ont recours aux éléments présentant cette vulnérabilité. Souvent, les acteurs ne disposent pas de listes des divers éléments sur lesquels s'appuient leurs solutions. Et quand bien même ils disposeraient d'un inventaire, celui-ci ne peut pas tout prévoir.* »

Les failles, en effet, peuvent être de diverses natures. Les technologies, en outre évoluent sans cesse, pouvant donner lieu à de nouvelles vulnérabilités. « *Chacun doit se dire que, tôt au tard, ses systèmes pourraient présenter une vulnérabilité et être impactés. Au niveau de son approche en cybersécurité, ce qu'il faut challenger, c'est dès lors sa capacité à détecter, réagir et répondre à un incident* », explique Olivier Antoine.

Adopter une nouvelle approche

D'une part, il faut pouvoir s'appuyer sur une équipe capable d'identifier les failles et les risques, comme le fait un Security Operations Center, d'autre part, il faut se préparer à faire face à une attaque, quelle que soit sa nature. « *La protection périmétrique, qui vise à placer des remparts autour de ses systèmes, comme cela a été beaucoup fait jusqu'alors, ne fonctionne pas,* explique Jean-Marie Bourbon, Head of CyberForce Offensive Security au sein de POST Luxembourg. *Il faut aujourd'hui envisager d'autres approches, en commençant par se demander si on est effectivement prêt à réagir à toute éventualité. Les bonnes procédures sont-elles en place afin de pouvoir contenir l'attaque, limiter la casse ou, le cas échéant, restaurer les systèmes ou les données ?* »

Faisant face à des menaces de plus en plus sophistiquées, les entreprises doivent donc se préparer. Tôt ou tard, elles devront gérer une crise. Les experts de POST Cyberforce sont formels, toute personne qui souhaite vraiment compromettre une infrastructure parviendra d'une manière ou d'une autre à ses fins. A côté de cela, les entreprises sont sous le feu permanent d'attaques plus opportunistes mais néanmoins bien pensées. A ce niveau, les tentatives de phishing sont de plus en plus élaborées, dans le but de tromper l'utilisateur et de récupérer des informations.

L'humain, l'autre grand vecteur d'attaque

« *Les principaux vecteurs d'attaque, aujourd'hui, ce sont les vulnérabilités Zero Day d'une part, et le facteur humain d'autre part, à travers les tentatives de phishing,* explique Régis Jeandin, Head of CyberDefense au sein de POST Luxembourg. *Entre 2020 et 2021, de plus en plus d'attaques exploitant de nouvelles vulnérabilités ont été menées. On parle d'une croissance de plus de 200%. Etant donné l'importance du facteur humain, il est primordial d'éduquer et de sensibiliser toutes les équipes. Toutefois, l'erreur humaine ne pouvant être éradiquée, le risque de compromission par ce vecteur reste important. Toutefois, le risque de compromission, dans la mesure où l'erreur est humaine, reste important.* » Des exercices régulièrement menés dans les entreprises, pour tester les collaborateurs et les sensibiliser, viendront en témoigner. Au sein d'une équipe, il y a toujours un utilisateur pour, au moins, cliquer sur un lien envoyé dans un e-mail frauduleux.

S'entrainer et se tester

Face à une possibilité d'attaque, toute organisation doit s'entrainer et tester ses systèmes autour de scénarios réalistes. Une RED TEAM, par exemple, aura pour mission de challenger les entreprises en considérant sa surface d'attaque réelle (et non un périmètre bien déterminé comme cela s'envisage avec un test de pénétration).

L'idée est d'exposer régulièrement l'entreprise à des exercices proches de la situation réelle, en simulant des attaques réalistes, qui pourront exploiter aussi bien la sécurité physique des bâtiments, l'informatique, le facteur humain à travers le phishing ou des approches de social engineering. « *De manière générale, les attaques peuvent être coordonnées, exploiter plusieurs points d'entrée, divers canaux, en vue d'atteindre un objectif,* explique Jean-Marie Bourbon. *Procéder à des tels exercices permet de tester la réaction, de voir l'efficacité des procédures en place, dans la perspective de pouvoir les améliorer. C'est comme pour un exercice incendie. Il faut pouvoir réfléchir à toute éventualité afin de pouvoir apporter une réponse efficace et coordonnée en situation de crise.* »

Sensibiliser les collaborateurs à distance

L'année 2021 a été une période encore fortement marquée par la COVID-19. De nombreux collaborateurs ont continué à travailler à distance. « *Le télétravail est contexte propice pour mener à bien des attaques de type « phishing »,* commente Régis Jeandin. *A la maison, où les frontières entre l'environnement professionnel et la sphère privée s'effacent, la vigilance à l'égard des menaces a tendance à s'estomper. On est moins vigilant. Pour les équipes en charge de la cybersécurité, il est difficile de gérer la sécurité jusqu'au domicile de chacun.* » Dans ce contexte, on a donc assisté à une recrudescence d'attaques de phishing. Dès lors, il est important de soutenir la communication, de renforcer la sensibilisation en rappelant les bonnes pratiques et les règles d'hygiène en matière de sécurité.

Multiplication des attaques sur mobile

« *On a aussi assisté à une hausse des tentatives d'attaques sur les téléphones mobiles,* commente Jean-Marie Bourbon. *A ce niveau, ce sont souvent des liens envoyés en message privé sur LinkedIn ou Twitter, qui permettent de récupérer des informations confidentielles contenues dans le téléphone. Les mobiles, qui contiennent aujourd'hui de très nombreuses et précieuses données, sont de plus en plus les cibles privilégiées des attaquants.* »

Les réseaux télécoms aussi sont ciblés

Les réseaux de télécommunication, d'autre part, peuvent aussi faire l'objet d'attaques. Pour y répondre, POST, en tant qu'opérateur historique dont les activités sont considérées comme critiques, prend les mesures appropriées. « *Cela se traduit par la mise en œuvre d'outils de détection avancés, permettant d'identifier des usages non conformes des cartes SIM que nous mettons à disposition, pour par exemple lancer une attaque de type phishing vers d'autres utilisateurs,* explique Alain Hirtzig. *A ce niveau, les techniques de fraude évoluent. Nous devons dès lors rester vigilants, pour contrer toute tentative visant à exploiter notre infrastructure ou nos services à des fins malveillantes.* »

En la matière, les équipes de POST Cyberforce ont beaucoup travaillé sur le déploiement de la 5G, qui soulève de nouveaux challenges en terme de sécurité. « *L'enjeu, pour nous, a été de créer un environnement securisé pour les utilisateurs du réseau de nouvelle génération,* poursuit Alain Hirtzig. *Pour cela, il faut pouvoir déployer des capacités de détection et de sécurisation dès la conception du réseau. Les évolutions technologiques nous poussent à aller plus loin. Par exemple, autour des enjeux relatifs à la 5G et à la sécurité, nous menons des projets de recherche, avec le LIST notamment, financés par le Ministère de l'Économie.* »

Aller toujours plus loin

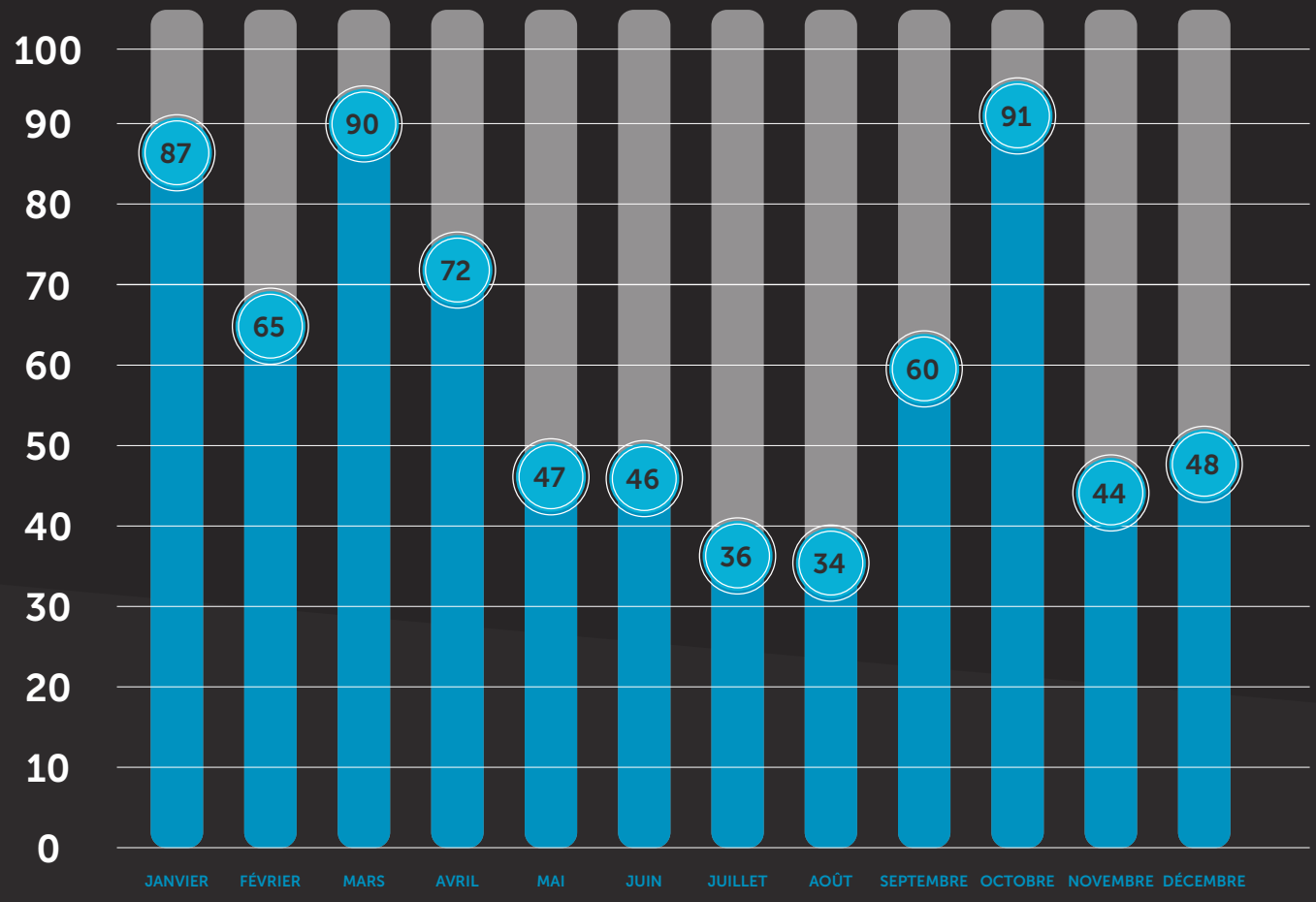
Un autre projet est mené avec l'ESA. Son objet est de garantir la confiance dans les échanges en attestant de l'authenticité du contenu partagé et des interlocuteurs (lire notre article relatif à Proofile, cf page 26).

« *En permanence, notre équipe cherche à proposer des solutions avancées de sécurité et des services contribuant à soutenir nos clients face à des attaques ou à les y préparer,* explique Olivier Antoine. *Cela se traduit par des technologies avancées de détection des anomalies, notamment au niveau de l'équipe de «Defensive Security», ou encore par des simulations d'attaque d'envergure, pouvant croiser plusieurs problématiques, pour évaluer la résilience de chacune. Ce sont des approches découlant de ce qu'on pourrait appeler une « jurisprudence Fukushima ». D'autre part, les projets de recherche visent à créer de la valeur à long terme, à nous emmener plus loin, à étoffer notre portefeuille de solutions.* » Enfin, acteur critique au Luxembourg, l'équipe de POST Cyberforce est engagée dans des actions de coopération au niveau national et européen, pour renforcer la réponse à toute attaque coordonnée contre notre société et améliorer la régulation internationale en matière de cybersécurité.

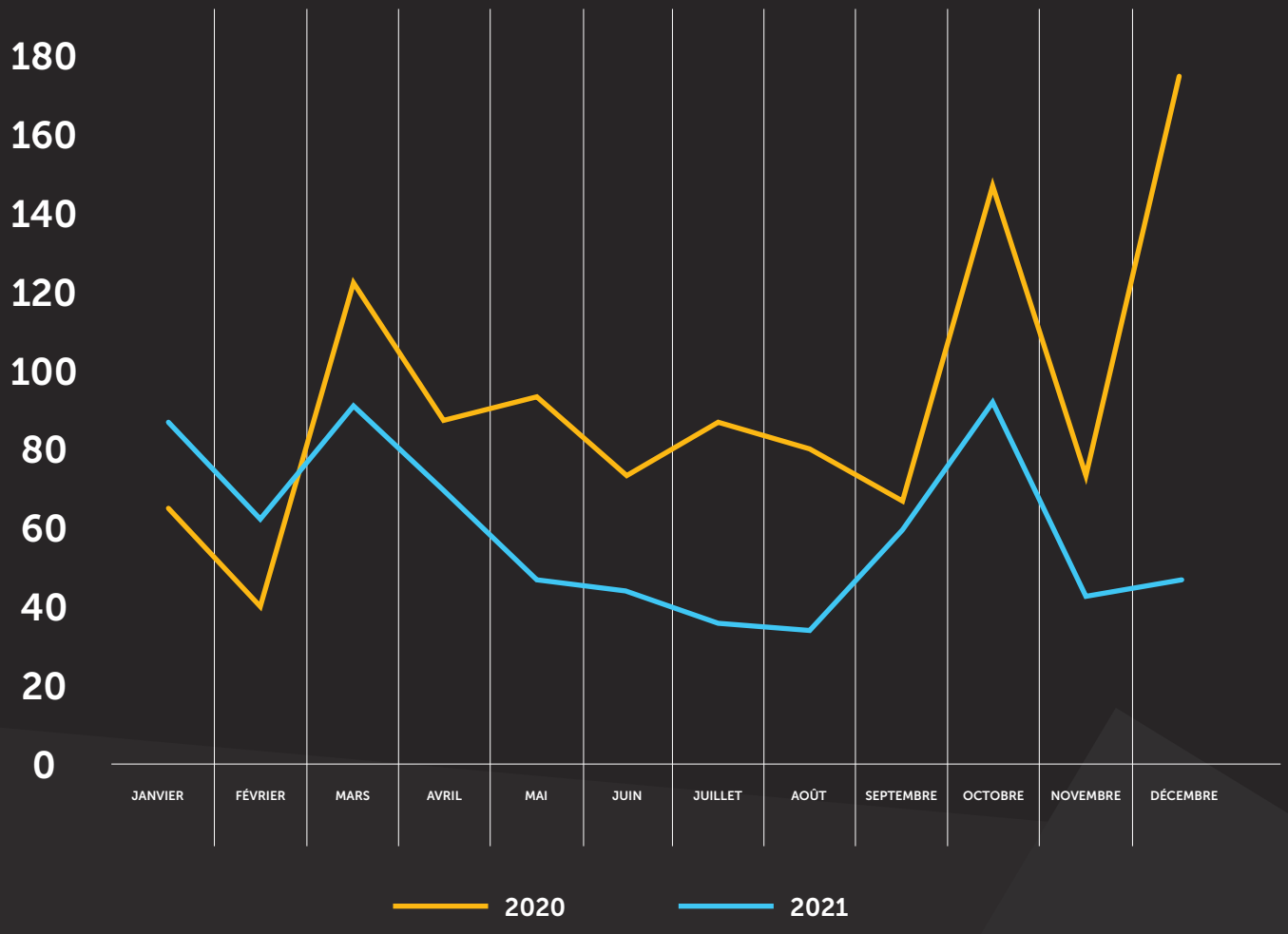
STATISTIQUES

Retour sur les attaques principales détectées en 2021 par l'équipe CSIRT de POST Cyberforce.

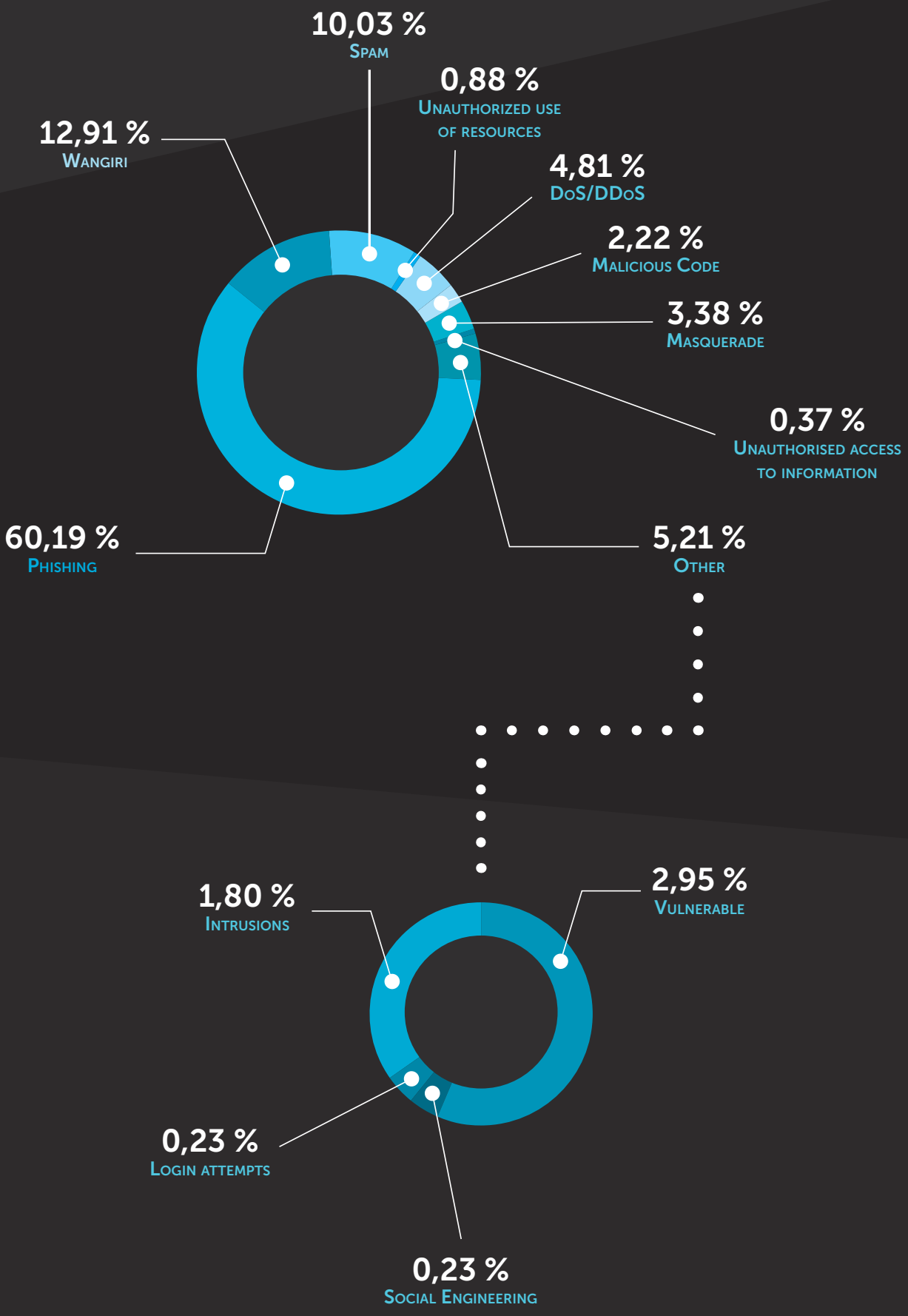
NOMBRE D'INCIDENTS DE SÉCURITÉ ENRÉGISTRÉS EN 2021



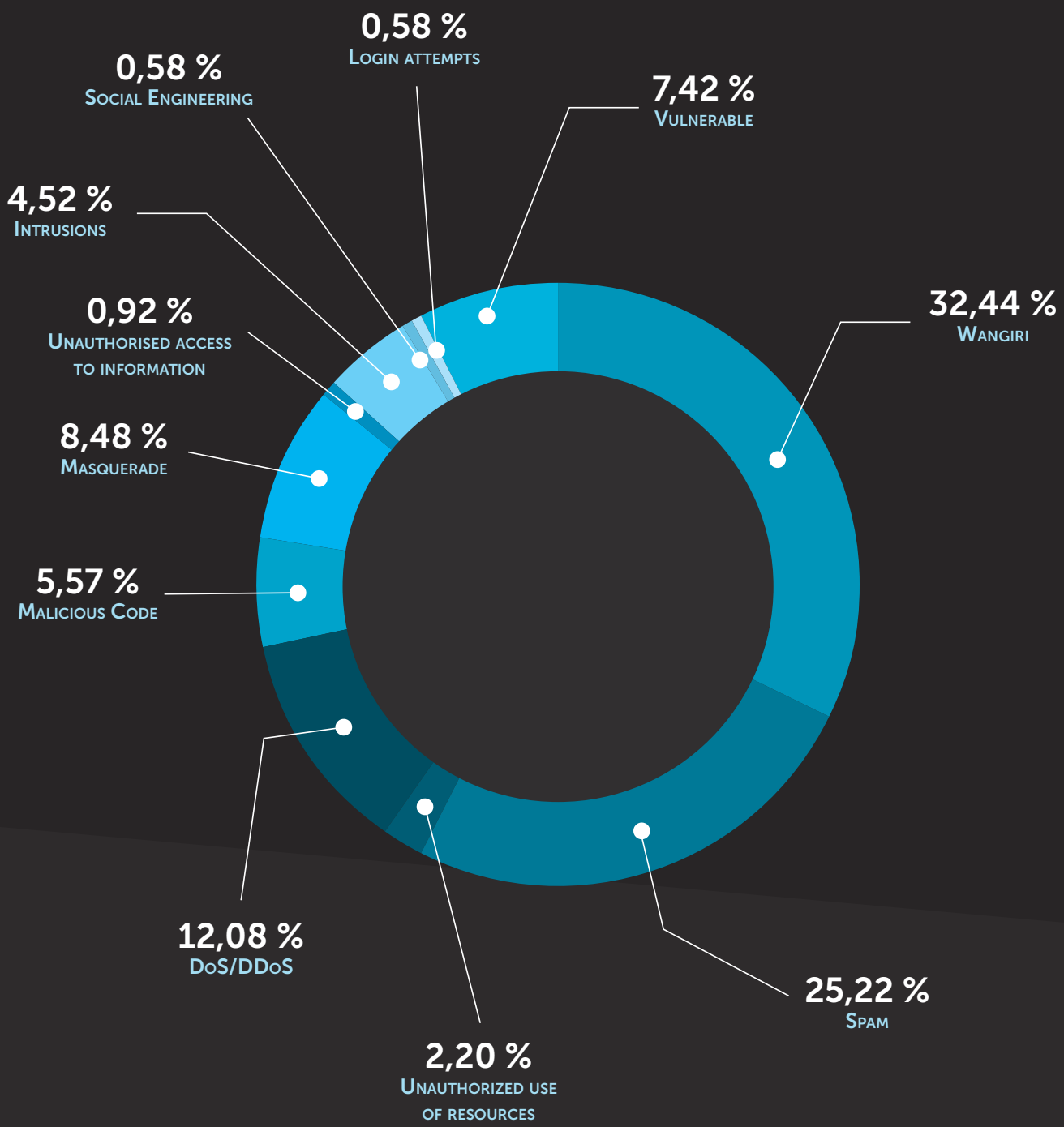
COMPARAISON DES INCIDENTS DE SÉCURITÉ DÉTECTÉS 2020 VS 2021



INCIDENTS DE SÉCURITÉ 2021



RÉPARTITION SANS LE PHISHING



Tendances 2021

Retour sur les tactiques et techniques les plus utilisées par les acteurs malveillants.

Obtention d'un accès initial

Au cours de l'année 2021, sur l'ensemble des incidents de sécurité observés, POST Cyberforce a pu dresser un classement des techniques les plus utilisées par les acteurs malveillants pour obtenir un accès initial en vue de compromettre un système.

Classement des techniques préférées des acteurs malveillants :

1. Phishing

Le phishing demande un effort de reconnaissance assez faible, en se basant notamment sur des données de sources ouvertes (OSINT), et permet de passer l'étape de l'accès initial assez rapidement en vue d'atteindre l'objectif recherché. Points faibles de cette technique cependant : son manque de discrétion et l'emploi de ressources importantes pour l'élaborer (domaine, hébergeur, site web, etc...).

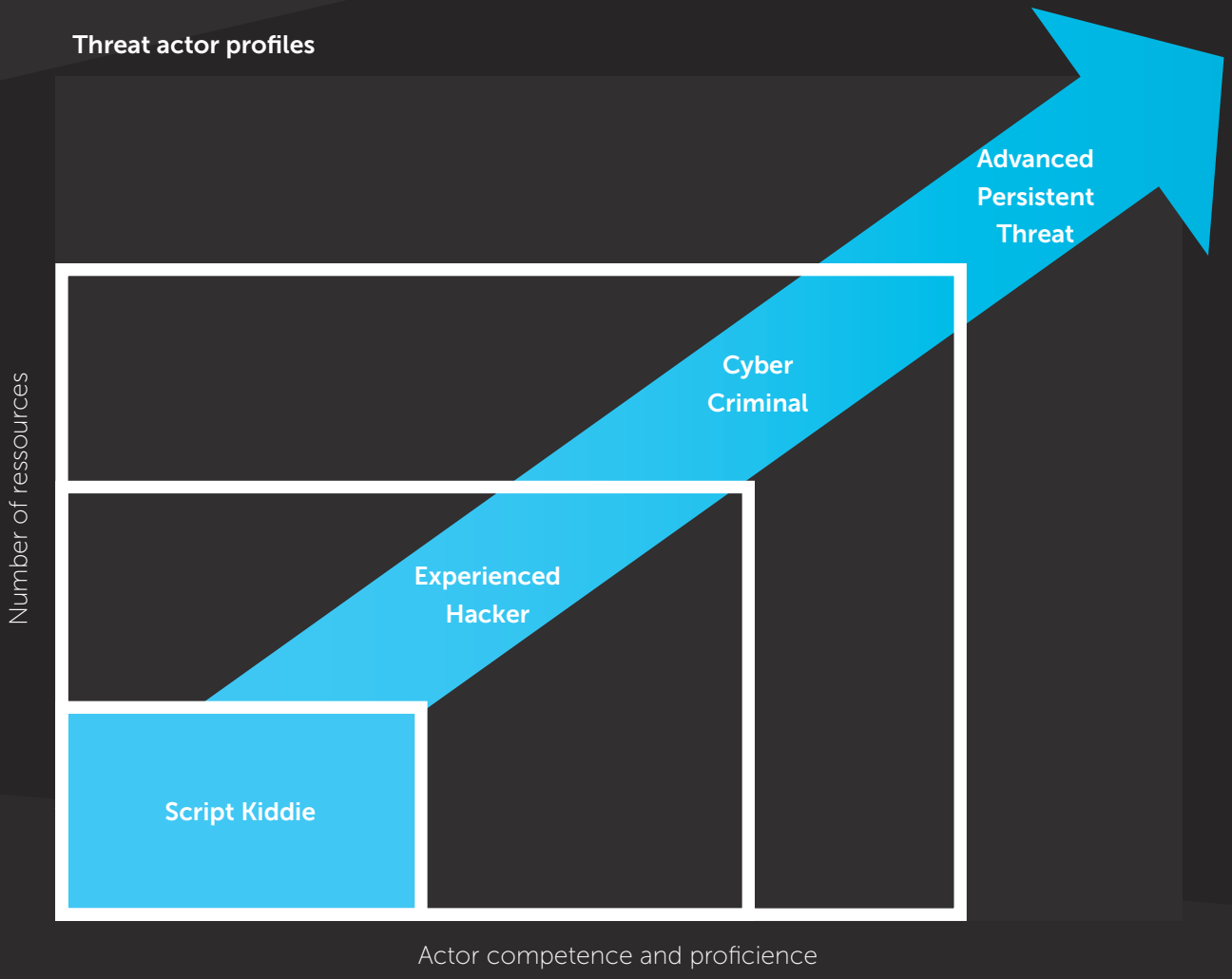
2. Exploitation d'une vulnérabilité connue

Elle a l'avantage de rester discrète selon le degré de maturité de la victime (Absence d'alerte d'intrusion ou de système de détection ou de prévention d'intrusion) et permet de s'introduire au cœur des systèmes. L'inconvénient principal réside dans le caractère opportuniste de cette technique. En effet, lors de la publication de vulnérabilités connues et de la disponibilité des exploits (logiciels permettant de réaliser une intrusion), selon la réactivité de la victime à mettre à jour ses systèmes, les acteurs malveillants doivent agir rapidement afin d'augmenter leur chance de succès. De plus, elle nécessite un effort de reconnaissance supérieure au phishing afin de vérifier si la vulnérabilité peut être exploitée par un moyen particulier.

3. Data breach

L'exploitation de données issues d'une fuite permet également de récupérer des identifiants de comptes ayant fait l'objet d'une fuite. Il s'agit dans ce cas précis, d'exploiter un fichier, appelé plus familièrement « leak », en vue d'attaquer la victime cible. Cette technique a l'avantage d'obtenir des identifiants en toute discrétion en vue d'attendre l'objectif cible d'un acteur malveillant plus rapidement. L'exploitation de ces fichiers s'effectue via des attaques du type «credential stuffing», c'est-à-dire de tester tous les identifiants du fichier vers un système ou une application pour tenter de vérifier si des comptes sont exploitables pour un accès à un système ou une application donnée. L'inconvénient majeur de cette technique réside dans la disponibilité du fichier. En effet, ces données sont rarement disponibles publiquement puisqu'elles sont échangées entre acteurs malveillants moyennant des finances en crypto-monnaie sur le darknet. Cette technique est réservée à des profils particulièrement avancés tels que ceux issus du crime organisé.

Enfin, la dernière technique, certainement, la plus élaborée qui se présente, est l'accès initial par la chaine d'approvisionnement (Supply chain attack). Cette technique fut utilisée fin 2020 à travers la compromission du logiciel SolarWinds Orion ou lors de la compromission du logiciel Kaseya VSA. Cette technique, bien que discrète, consiste à compromettre, non pas directement la victime mais son fournisseur de logiciels par l'intrusion d'un code malveillant lors du développement de mise à jour. Une fois que la victime a mis à jour son logiciel, l'acteur dispose d'un accès initial au cœur de l'organisation. Cette technique présente l'avantage d'obtenir un accès initial en toute discrétion. Cependant, elle nécessite de compromettre en premier lieu un éditeur de logiciels ce qui complexifie l'effort et les chances d'atteindre l'objectif. Selon nos observations, ces techniques sont utilisées par des profils particulièrement avancés.



Profil des acteurs malveillants en fonction de leurs compétences et de leurs capacités.

Zoom sur le phishing

Cette année encore, le phishing reste dans la tendance des techniques les plus utilisées par les acteurs malveillants pour atteindre leur cible.

Issue des tactiques permettant d'obtenir un accès initial, cette technique permet d'atteindre directement la dernière ligne de défense, à savoir, l'utilisateur. Comme en 2020, tous les moyens sont bons pour atteindre une victime : réseaux sociaux, email ou SMS.

Procédé ordinaire

Particuliers ou entreprises, le procédé est identique :

- L'envoi d'un message, qu'il s'agisse d'un email ou un SMS, alertant sur des modifications nécessaires sur le compte de la victime;
- La présence d'un lien sur lequel l'utilisateur est invité à cliquer;
- Après avoir cliqué sur le lien, la présence d'un site web invitant les utilisateurs à entrer leurs identifiants. Les pages web utilisées dans ce cadre sont appelées « kits de phishing »;
- Après que la victime ait introduit ses identifiants, un email est envoyé depuis le kit vers l'adresse email de l'acteur malveillant ou ce dernier va pouvoir exploiter cette ressource.

Nouvelles techniques

L'utilisation de divers raccourcisseurs d'URLs (bit.do, urlz.fr, rebrand.ly...), est aussi une opportunité pour les attaquants de cacher des URLs suspectes derrière des domaines légitimes. Les URLs trop longues sont tout de suite considérées comme suspectes.

Entreprises

Les entreprises ont été victimes, tout au long de l'année de campagne de phishing particulièrement ciblées, appelées également « Spearphishing ». Les accès souhaités par les acteurs malveillants sont principalement les comptes de collaborateurs. Appelés également comptes AD (Active Directory), ils permettent à un collaborateur d'accéder à l'ensemble des ressources de l'entreprise.

Avec de plus en plus d'entreprises ayant recours à la déportation de leur infrastructure au sein de services cloud, les acteurs malveillants ciblent donc ces entreprises en vue d'obtenir ces identifiants depuis leur espace cloud Microsoft Azure. Ainsi, il leur est parfaitement possible d'obtenir des accès initiaux vers le Webmail d'entreprise ou de disposer d'un accès directement à l'infrastructure de l'entreprise en vue de subtiliser des documents ou tout autre actif d'intérêt.

Particuliers

Comme en 2020, les clients résidentiels furent la cible de campagne de phishing de type « bulk » c'est-à-dire, l'envoi en masse de messages sans distinction d'un destinataire particulier. Un des objectifs de ces campagnes est de subtiliser des identifiants issus de moyens de paiement qu'il s'agisse des identifiants d'une carte bancaire ou d'un espace numérique bancaire en vue de perpétrer une fraude ultérieure. En 2021, l'usurpation des moyens authentifications (LuxTrust), d'un colis à aller récupérer ou l'usurpation des banques elles-mêmes furent des techniques particulièrement exploitées pour obtenir ces précieuses informations.

En ce qui concerne les clients résidentiels, l'autre objectif cible des acteurs malveillants sont les identifiants de comptes emails. En effet, une adresse email étant le centre de l'ensemble des échanges avec d'autres services, un compte email permet de rebondir sur d'autres identifiants supplémentaires par recherche dans l'historique des emails et par demande de réinitialisation de compte emails. Au cours de l'année 2021, POST Cyberforce a été témoin d'un acteur malveillant ayant subtilisé les identifiants d'un compte email d'une victime pour supprimer les emails, changer les mots de passe et les comptes de l'ensemble des services en ligne (Services cloud) et réseaux sociaux (Facebook, Instagram, Twitter, etc....) tout en demandant une rançon à la victime pour lui permettre de retrouver ses comptes.

Vishing / Call SPAM

En plus des phishings envoyés par messagerie texte, la résurgence de récupération d'identifiants par appel téléphonique a été particulièrement marquante en 2021. Qu'il s'agisse d'usurper l'identité d'entreprises comme Microsoft ou de la police, l'objectif reste identique : subtiliser des identifiants en vue de réaliser une fraude.

Ces campagnes malveillantes ont été particulièrement nuisibles à travers un nombre important d'appels téléphoniques.

Une des campagnes mémorables de l'année fut l'usurpation d'un service client Microsoft prétendant que l'ordinateur de la victime fut rempli de virus et logiciels malveillants en tous genres. Le procédé profite de la crédulité des victimes afin de leur faire installer un outil de prise de contrôle à distance et de récupérer toutes les informations tapées au clavier par la victime dont les identifiants d'accès aux comptes bancaires.

Ainsi, la lutte contre ce phénomène s'accompagne d'une meilleure sensibilisation du plus grand nombre à ce type d'approche utilisée par les acteurs malveillants, aussi bien pour les entreprises que pour les clients résidentiels.

Vulnérabilités

2021 a été l'année de la présence et de l'exploitation de systèmes vulnérables à forte surface d'attaque, c'est-à-dire, dont la présence sur internet est très vaste.

Le début d'année a été marqué par HAFNIUM portant sur les serveurs équipés de versions de Microsoft Exchange 2013, 2016 et 2019 vulnérables à l'exécution de code à distance. Une exploitation de cette vulnérabilité peut conduire un acteur malveillant à profiter des ressources des serveurs qu'il s'agisse de miner de la cryptomonnaie ou de renvoyer des courriels malveillants (Phishing, code malveillant) à d'autres victimes potentielles ou d'extraire des données issues des courriels.

En 2021, une vulnérabilité a été divulguée concernant le spouleur d'impression Windows. Cette vulnérabilité permettrait de réaliser pour les versions affectées une exécution de code à distance (RCE), c'est-à-dire une prise de contrôle par un acteur malveillant de l'environnement où sont installés les spouleurs vulnérables.

La vulnérabilité Log4Shell a marqué cette fin d'année et a mis à rude épreuve les équipes IT et les équipes de cybersécurité. Cette vulnérabilité permet, à tout équipement dans lequel une version vulnérable du logiciel Log4j est installée, de prendre un contrôle sur l'équipement pourvu qu'un acteur malveillant puisse disposer d'une connectivité vers le serveur. La mise en lumière d'une vulnérabilité présente sur des millions de serveurs dans le monde a grandement contribué à la découverte successive de plusieurs vulnérabilités en cascade.

De manière générale, le nombre de vulnérabilités augmente depuis 2017.

Data breach

L'actualité a été particulièrement riche sur ce type d'évènements au cours de l'année 2021. Bien qu'une grande majorité du spectre de la menace se situe en dehors des frontières du Grand-Duché, les fuites de données associées ont parfois des répercussions jusqu'au Luxembourg.

Ainsi, nous pouvons citer la publication des scrapings sur les réseaux sociaux tels que Facebook, Instagram et LinkedIn d'avril à juillet 2021. Bien moins intrusifs qu'une fuite de donnée pure et simple, le scraping est une technique consistant à rassembler des données personnelles issues de pages publiques sur les réseaux sociaux. Les données collectées par les acteurs malveillants sont ensuite exploitées pour perpétrer des campagnes de phishing personnalisées aussi bien vers les profils dont l'adresse email a pu être récupérée que vers les mobiles à travers l'envoi de SMS de phishing par exemple.

En septembre, POST Cyberforce a été témoin d'une fuite de données issue de l'exploitation d'une vulnérabilité Fortinet en 2018 (CVE-2018-13379) par des acteurs malveillants ayant pu récupérer près de 500 000 comptes d'accès aux équipements du type pare-feu associés à des adresses IP. Parmi ces adresses IP figuraient des adresses IP luxembourgeoises. Ce type de fuite de données nous rappelle l'importance de disposer d'une fréquence de changement de mots de passe régulière, en particulier, pour des comptes techniques exposés sur Internet.

Intrusions

Bien souvent issues d'accès initiaux ayant réussi, une fois qu'un acteur malveillant s'est introduit dans un système ou une application, l'objectif à atteindre est à la portée de ce dernier.

POST Cyberforce a été témoin d'intrusions sur des comptes emails, tout comme sur des applications web. Ces intrusions ont permis, la plupart du temps, de réaliser de nouvelles fraudes ou de réutiliser les serveurs soit pour réaliser des opérations de défacement, soit pour exploiter à nouveau les ressources du serveur afin de miner de la crypto-monnaie de type Bitcoin.

POST Cyberforce a également été témoin de la propagation de bots exploitants des vulnérabilités propres à des plugins de Wordpress afin de s'y installer et d'attaquer d'autres serveurs Web utilisant des plugins de Wordpress vulnérables.

Codes malveillants

De multiples familles de logiciels malveillants ont été utilisées pour perpétrer des attaques aussi bien vers les entreprises que vers les clients résidentiels. Ces logiciels sont bien souvent utilisés pour permettre à un acteur malveillant de prendre le contrôle sur une machine distante. Ce type de logiciel malveillant est plus connu sous le nom de R.A.T. soit « Remote Access Trojan », c'est-à-dire des chevaux de Troie, usurpant l'identité de logiciels connus dissimulant un code malveillant permettant de prendre le contrôle sur une machine distante par un acteur malveillant.

Par ce procédé, ce dernier peut atteindre plus facilement son objectif de perpétrer une fraude ou de procéder à un vol de données. Dans le cadre de ce rapport, deux types sont mis en évidence :

- Les chevaux de Troie bancaires (Flubot Mobile Trojan ou Medusa)
- Les enRégistreurs de frappe (Keylogger de type Agent Tesla ou Nanocore)

Concernant les chevaux de Troie bancaires, Flubot a la particularité d'être utilisé sur des réseaux mobiles. En effet, il s'est largement propagé à travers le réseau mobile. Une fois le téléphone Android infecté, celui-ci est ensuite capable d'envoyer des SMS vers les prochaines victimes à partir de la liste de contact du mobile infecté et ainsi de suite.

En ce qui concerne les enRégistreurs de faute de frappe, le cheval de Troie Agent Tesla est vendu comme étant un Malware-as-a-Service (MaaS) au sein des marchés noirs sur le darknet dont un support est disponible en permanence.

Sa facilité d'utilisation permet à des attaquants novices de mettre en place très rapidement des attaques. Ce code malveillant est aussi intéressant de par son coût relativement faible. Ce qui n'est pas négligeable lorsque les attaquants recherchent un retour sur investissement suffisant.

Masquerade

Le volume d'attaques par usurpation d'identité a été relativement contenu au cours de l'année. La manifestation des usurpations d'identité sur les réseaux sociaux se confirme. En effet, les entreprises continuent à être victimes de ce type d'incident visant les utilisateurs des réseaux sociaux. L'objectif est de pouvoir récupérer des identifiants de connexion à des comptes bancaires, des comptes sur les réseaux sociaux ou des numéros de téléphone en vue de les faire souscrire à des abonnements SMS premium en incitant l'utilisateur à entrer son numéro mobile.

Du côté des fraudes au président, bien que la tendance a été pendant longtemps de fournir, de la part des acteurs malveillants, leur numéro de compte bancaire, désormais les acteurs malveillants demandent l'achat de cartes cadeaux (Gift card Apple par exemple). Cette technique permet à un acteur malveillant d'éviter de divulguer des numéros de comptes bancaires et donc de donner des pistes éventuelles pour être retracé.

Pour les profils du type « cyber criminels », les techniques d'usurpation sont tellement perfectionnées qu'ils vont même jusqu'à usurper les noms de domaine des entreprises ciblées. Ce qui nécessite une vigilance accrue pour faire face à ce type d'incident.

ZOOM SUR LES ATTAQUES DDoS DETECTEES PAR CYBERFORCE EN 2021

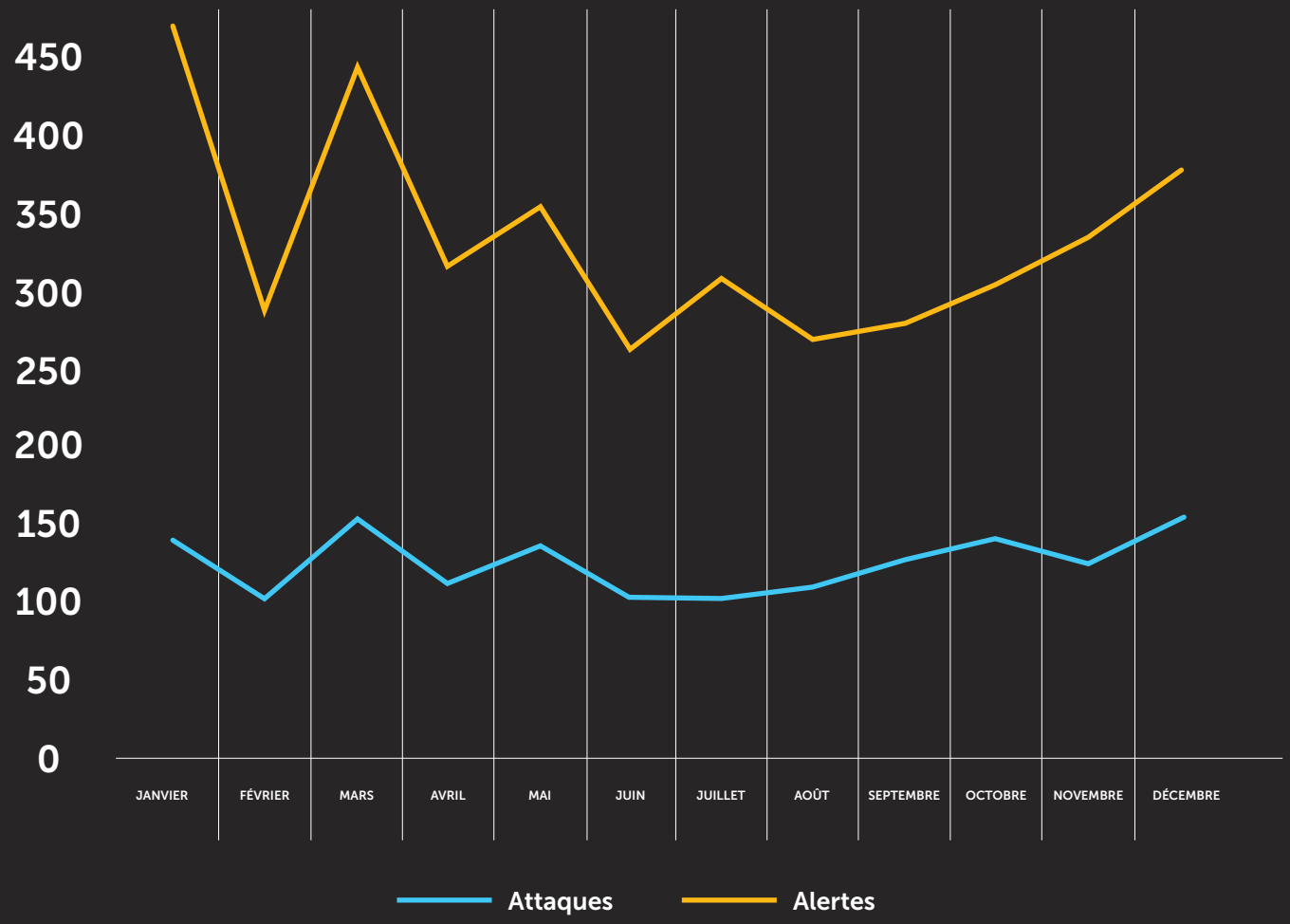
Les attaques DDoS visent à rendre indisponible un serveur, un service ou une infrastructure informatique et télécom en surchargeant la bande passante du serveur ou en monopolisant ses ressources jusqu'à épuisement, entraînant une impossibilité pour vos clients et employés d'accéder à vos services Internet.

En 2021 les attaques volumétriques ont été plus intenses qu'en 2020 avec respectivement 16 Gbps au 1er trimestre et 21 Gbps au 4ème trimestre.

Top 4 des types de distribution d'alertes :

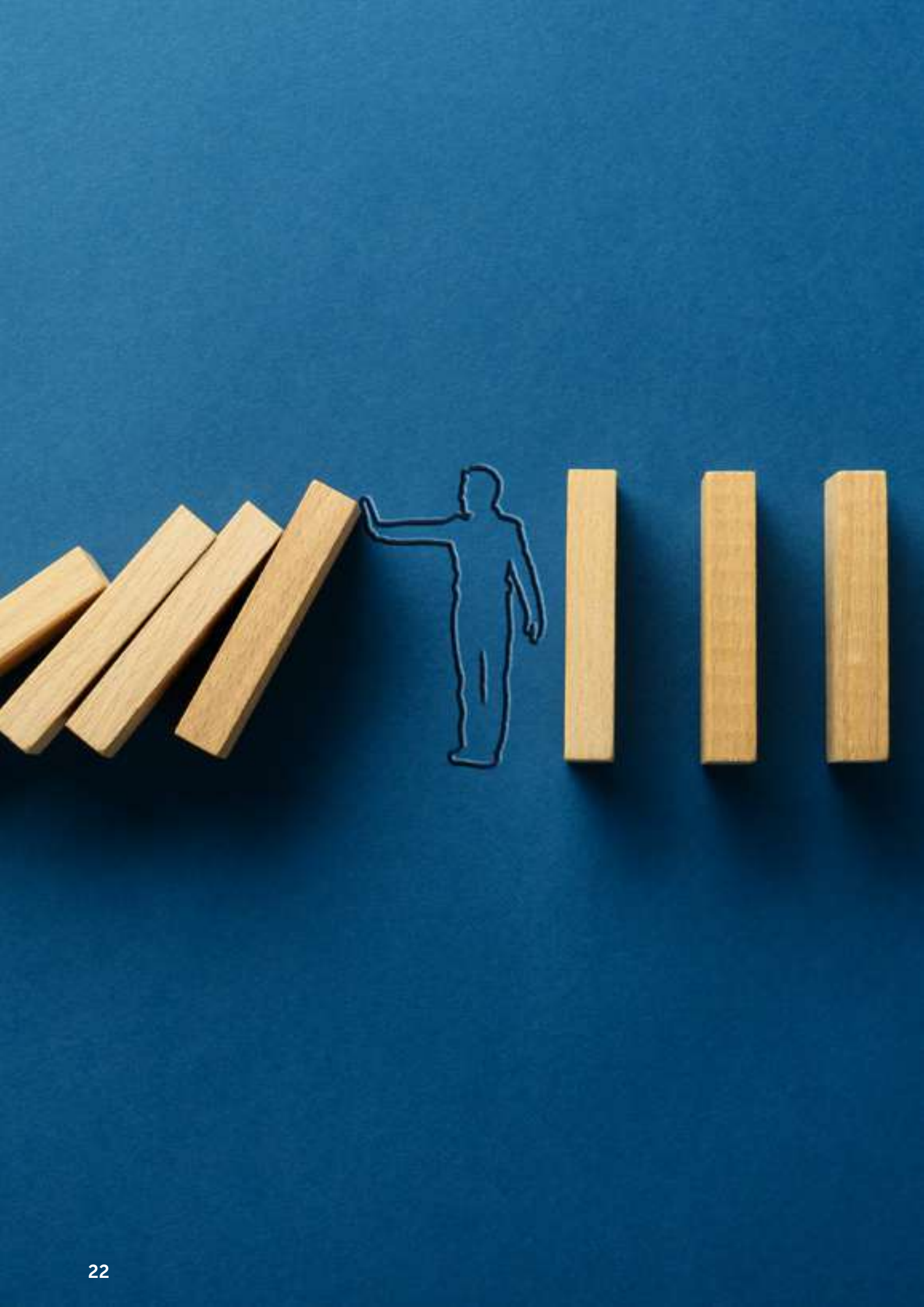
- DNS Amplification
- UDP Flood
- ACK Flood
- QUIC Flood

Nombre d'attaques et d'alertes détectées par POST Cyberforce – 2021



Bien que la plupart des attaques DDoS restent sous contrôle, grâce notamment aux solutions proposées par les opérateurs, ce type d'incident reste d'actualité et la vigilance doit être maintenue afin de se prémunir de ce type d'attaque. Les opérateurs de télécommunications peuvent fournir de plus amples informations et conseiller les entreprises afin de trouver la meilleure solution adaptée à leur besoins. POST Telecom peut, grâce à son service anti-DDoS vous protéger contre ce type d'attaque.

Retrouvez chaque mois les statistiques relatives aux attaques DDoS détectées au Luxembourg sur le blog https://ictexpertsluxembourg.lu



LA RÉSILIENCE ET LA GESTION DE CRISE AU COEUR DE TOUTES LES PRÉOCCUPATIONS

FOCUS : VOTRE ORGANISATION EST-ELLE PRÊTE ?

POURQUOI EST-IL IMPORTANT D'AVOIR UN PLAN DE CONTINUITÉ D'ACTIVITÉ ?

Au cours des dernières années les entreprises ont eu à traverser des crises de plus en plus soudaines, variées et avec un fort impact pour leurs activités. Outre la pandémie de la COVID-19 avec ses contraintes de déplacement et le repli économique qui s'en est suivi, les directions doivent faire face à la montée exponentielle des cybermenaces et l'apparition des risques liés au réchauffement climatique pour ne citer que les plus importants.

Pouvoir évoluer dans un monde incertain est une condition de survie qui pousse les entreprises à développer ou revoir à la hausse leurs **Plan de Continuité d'Activité-PCA / Plan de Reprise d'Activité-PRA** et s'assurer d'un niveau de résilience idéal.

Définition du plan de continuité d'activité : Le PCA va bien au-delà du seul aspect IT

Les projets de PCA (Plan de Continuité d'Activité) et de PRA (Plan de Reprise d'Activité) sont souvent abordés comme des projets IT uniquement, or ces approches doivent couvrir l'ensemble des activités et des processus qui constituent le métier de l'entreprise, les systèmes informatiques mais aussi les fournisseurs d'énergie, de logistique et des locaux où les employés pourront reprendre le travail si ceux de l'entreprise ne sont plus praticables.

Le plan de continuité d'activité, un concept éprouvé

Le concept de continuité d'activité est éprouvé. Apparu dans les années 80, il adressait une partie de la problématique avec les plans de reprise d'activités (ou disaster recovery plans). Les efforts portaient essentiellement sur l'informatique, avec la volonté de garantir la disponibilité des systèmes ou permettre leur remise en fonction rapide après un incident. C'est avec la publication de la norme BS 25999 et l'établissement de la certification ISO 22301, que le concept a été élargi. Désormais, les projets relatifs à la continuité d'activités couvrent un spectre étendu. Ils sont portés par le board, en considérant l'activité avec une approche holistique.

Guide pour élaborer un plan de continuité : 5 règles à respecter

Règle n° 1 : Partez du métier pour évaluer les impacts

C'est en considérant le métier que l'analyse doit se construire, en prenant en compte l'ensemble des facteurs qui peuvent nuire à la bonne marche de l'activité. Ces enjeux dépassent de loin la gestion des systèmes en commençant par identifier les activités essentielles à l'organisation ou à travers une meilleure compréhension des processus, pour ensuite effectuer une analyse d'impact. Il est important de comprendre quels pourraient être les effets de l'arrêt d'un processus critique dans le temps et sur l'ensemble de l'activité.

Cette première étape relève du Business Impact Analysis. Elle ne peut être conduite qu'en menant une étude approfondie de l'ensemble des départements constituant l'organisation pour identifier les activités entreprises et la manière dont chacun prend part aux procédures.

Règle n° 2 : Identifiez les activités critiques et évaluez le niveau de tolérance à l'interruption

A travers les entretiens menés, identifiez les activités critiques, les liens d'interdépendance existants vis-à-vis d'autres départements ou d'acteurs externes. Dans chaque département et direction, challengez les équipes. Au départ d'un framework établi au regard de notre expérience et des bonnes pratiques reconnues, évaluez également les effets d'une interruption de l'activité au niveau de chaque équipe selon différents critères comme le Recovery Time Objective (RTO), le Recovery Point Objective (RPO), le Maximum Acceptable Outage (MAO) ou encore le Minimum Business Continuity Objective (MBCO). A travers ces indicateurs, on relève ce qui est acceptable en termes d'interruption pour chaque département, et ce jusqu'à la capacité réelle de l'IT à supporter les métiers.

Règle n° 3 : Alignez les besoins au service du business

Parce que, d'un département à l'autre, les perceptions de ce qui est acceptable peuvent diverger, un des objectifs sera de réconcilier les sensibilités au regard des besoins réels du métier. « Dans la plupart des cas, c'est au sommet de l'entreprise que les arbitrages ont lieu, le top management étant souvent le seul à pouvoir statuer vis-à-vis des risques encourus. Le management rationalise et décide souvent par rapport au niveau d'exposition admissible des affaires, donc du secteur d'activité et de la clientèle de l'entreprise, en cas d'incident majeur. Pour l'obtention d'une certification liée à la continuité d'activités, il est indispensable de réconcilier l'ensemble des besoins des équipes autour d'un processus critique.

Règle n° 4 : Evaluez les processus afin de retenir les meilleures solutions

L'analyse de l'impact business est au cœur de toute démarche relative aux enjeux de continuité d'activités. Elle sera complétée par une analyse des risques. Celle-ci se traduit par l'identification des menaces pouvant conduire à l'interruption d'une activité jugée critique et par l'évaluation de la probabilité de leur survenance. Si une entreprise considère l'ensemble de ces éléments, alors des scénarii et des plans de reprise de l'activité dans les meilleurs délais peuvent être imaginés selon les différents cas de figure. Prenons les processus par exemple, soumettez-les à la menace afin d'envisager les solutions à mettre en place, comme la relocalisation des collaborateurs ou un plan de redéploiement des systèmes des garanties relatives à la restauration des lignes de télécommunication, sans oublier d'évaluer le niveau de résilience de vos fournisseurs critiques.

Règle n° 5 : Simplifiez-vous la vie. Tirez parti de la certification ISO 22301

La certification ISO 22301 a été élaborée spécialement afin de permettre aux organisations de s'inscrire dans une démarche d'amélioration continue : c'est un cadre standardisé idéal pour démarrer. L'enjeu principal est de mieux protéger l'activité dans sa globalité, par une meilleure compréhension des processus et des risques, et de s'assurer de sa robustesse avec l'ensemble des parties prenantes tels que les clients, les partenaires ou encore le régulateur de l'entreprise. Une telle certification est de nature à rassurer, à garantir la confiance vis-à-vis de la tenue des activités. EBRC accompagne des institutions actives dans le secteur de la finance, des banques, de l'industrie et de l'assurance pour l'obtention de cette certification.

Enfin, distinguer le risque de la menace pour réussir son plan de continuité d'activité

Beaucoup d'acteurs confondent risque et menace. Il est toutefois important de les distinguer. La menace est un élément bien particulier, une occurrence parfaitement identifiable. Il peut s'agir de la divulgation d'informations, une tentative de corruption, une intrusion dans des systèmes informatiques ou encore un acte terroriste. Cette menace peut s'abattre plus ou moins facilement sur un processus, en fonction des vulnérabilités qu'il présente.

Pour évaluer le risque, il faut identifier la menace et définir la probabilité qu'elle affecte le processus. Il faut aussi évaluer l'impact de cette survenance probable sur l'activité, les finances, la réputation, ou encore vis-à-vis des obligations règlementaires. On obtient alors un niveau de risque faible, moyen ou important. Sur cette base et avec ces indicateurs, le dirigeant sera en mesure de définir l'objectif à atteindre : l'éliminer, le mitiger, voire l'accepter.

Testez la maturité de votre plan de continuité d'activité

Cette analyse complète est offerte gratuitement par EBRC, filiale du Groupe POST Luxembourg.

Florent Cochet
Créateur CoDare

INNOVATION

Garantir la confiance des échanges

En partenariat avec l'Agence Spatiale Européenne (ESA), le groupe POST met au point une solution visant à garantir l'authenticité des échanges et des documents numériques partagés. Baptisée Proofile, elle s'appuie pour cela sur des données de géolocalisation fournies par les satellites du programme Galileo ou encore par les réseaux télécoms.

Chaque jour, nous échangeons des documents et interagissons à distance avec de nombreuses personnes, le plus souvent connues, mais pas toujours. Face à la multiplication des fausses nouvelles, contre l'usurpation d'identité, alors qu'émergent les « deep fake », qu'est-ce qui vous permet de vous assurer que votre interlocuteur est bien celui qu'il prétend être ? Qui vous dit que l'on n'essaie pas de vous tromper ? Qu'est-ce qui vous garantit que le document qui vous parvenu est authentique, vrai, fiable ? A l'heure de la société numérique, la confiance dans nos interactions est devenue un enjeu fondamental.

C'est pour y répondre qu'est né, en 2019, le projet Proofile. « *A la suite d'un échange avec Pierre Zimmer, directeur général adjoint et Chief Strategy Officer, à propos notamment de la dynamique qui s'opère au Luxembourg dans le domaine spatial, nous avons mis en place une séance d'idéation, rassemblant les équipes d'InTech et de POST Luxembourg, dont les experts de POST Cyberforce,* explique Florent Cochet, project manager de Proofile, partner du cabinet de conseil CoDare. *A cette occasion, nous avons mené une réflexion autour des technologies connues et émergentes, dans le domaine spatial, de la cybersécurité et autour de la blockchain, en considérant les possibilités qu'elles offraient.* »

Lutter contre les « fausses nouvelles »

Après évaluation approfondie des 14 idées d'application qui en ont émergé, l'une d'elles a été retenue et a donné naissance au projet SkyTrust. « *Elle consistait à s'appuyer sur les données de géolocalisation émanant du projet Galileo de l'ESA, le concurrent européen au GPS américain, pour garantir la confiance des échanges entre personnes via les canaux de communication digitaux. Un des cas d'usage défendu au départ visait la lutte contre les fake news, avec l'idée de pouvoir prouver l'authenticité d'une photo prise en y associant les informations liées à la localisation du cliché et le moment auquel il a été pris* », poursuit Florent Cochet. C'est avec cette idée que le projet manager, s'appuyant sur l'expertise d'Intech pour le développement de la plateforme et sa maitrise de la technologie blockchain, et sur le savoir-faire de POST Cyberforce dans la sécurisation des échanges et des données, a frappé à la porte de l'Agence Spatiale Luxembourgeoise (LSA).

Un large champ d'application

« *En septembre 2019, nous présentons notre projet. Après une première itération, en janvier 2020, le LSA nous fait part de sa volonté d'avancer avec nous et nous demande d'obtenir des premières lettres d'intérêt de la part d'acteurs du marché.* » C'est alors que le groupe va à la rencontre de diverses organisations, explorant les cas d'usage tout en s'entourant d'autres acteurs pour affiner son projet. Il est notamment rejoint par l'Université de Luxembourg, pour mener un projet de recherche autour de l'utilisation des données et de l'intelligence qu'on peut en extraire. Il s'appuie aussi de l'expertise du DPO de POST ainsi que sur le département légal et le service marketing du groupe. « *Au-delà des entreprises média que nous avons approchées au début, et qui ont marqué un intérêt pour la solution, le monde financier nous a fait part de son enthousiasme pour la technologie, nous orientant vers d'autres applications,* poursuit Florent Cochet. *Un des enjeux, pour une grande partie des acteurs, est de sécuriser les échanges. Avec les données de géolocalisation, considérées comme des attributs d'identité, on peut garantir qu'un document ou qu'un message à bien été envoyé d'un endroit déterminé, où est censé se trouver notre interlocuteur, collègue, partenaire ou même client. Grâce à la blockchain, les éléments garantissant l'authenticité du document ou du message peuvent être conservés, avec la garantie qu'ils ne pourront pas être altérés.* »

Proofile

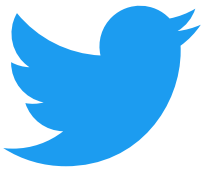
Un outil global, facilement accessible

La solution, rebaptisée «Proofile» entre temps, vient garantir la confiance des échanges, au même titre qu'une signature électronique. La grande différence, par rapport aux solutions d'e-signature, réside dans la facilité d'accès à la solution et l'intégration des critères de géolocalisation, s'appuyant sur le programme satellite Galileo ou encore sur des informations émanant du réseau télécom, pour s'assurer de l'identité de l'interlocuteur. « *C'est une solution globale, qui ne dépend pas des réglementations en place dans une région ou une autre. A ce titre, elle est facilement accessible. Pour chaque élément signé grâce à la plateforme, un QR Code est généré, permettant de vérifier les informations et d'apporter la confiance requise pour toute interaction* », explique Florent Cochet.

Un contrat signé avec l'ESA

Aujourd'hui, le projet Proofile est bien engagé. Le groupement, en février 2021, au terme de plusieurs itérations, a signé un contrat avec l'ESA. Aujourd'hui, le projet se poursuit, avec la mise à disposition de la plateforme, accessible en phase démo, via une interface web et à travers une application mobile, avec pour objectif de certifier rapidement de premiers échanges ou documents. Le développement de la solution, dans une démarche d'innovation, se poursuit, en même temps que l'équipe explore l'approche commerciale associée à son utilisation.

Be aware of new security incidents.



Follow us on Twitter

@CsirtPost

En cas de questions,
vous pouvez contacter nos experts
par email : **csirt@post.lu**
ou par téléphone : **8002 4000**

CYBERFORCE.lu