#EDENews

Edito – Guillaume Verney-Carron, Vice-président régional Auvergne Rhône-Alpes

PROTÉGEONS LE PATRIMOINE INFORMATIONNEL DE NOS ENTREPRISES

En 2023, plus que jamais, la question n'est plus de savoir ***SI*** nous allons être cyber-attaqués mais plutôt ***QUAND.*** En ce sens, il est important d'être au moins en mesure de minimiser (anti-virus, *anti-spam* et *anti-fishing*) et parer les attaques (*firewall* et autres systèmes de filtration), de les identifier en amont (*EDR*, *NDR XDR*…(*)) et d'être capable de remonter un système si celui-ci devait être affecté (sauvegarde sécurisée et plan de continuité d'activité).

Evidemment, tout cela a un coût qu'il convient de mesurer par rapport aux dégâts causés par une cyberattaque réussie. En d'autres termes, il est temps pour nos entreprises de prendre conscience de l'existence de cette menace, tenant compte de la criticité de nos secteurs d'activité et de nos technologies, et ne pas se cacher derrière une posture de « cyber-autruche ».

Nos donneurs d'ordre privés ou étatiques exigeront demain que nos entreprises soient protégées et préparées, d'où des exigences accrues et le déploiement des audits en cours.

Aujourd'hui le patrimoine informationnel de nos entreprises est plus que jamais dans nos systèmes d'information (SI) – Protégeons le, il le mérite.

(*) EDR : Endpoint Detection and Response , NDR : Network Detection and Response, XDR : eXtended Detection and Response

Save the date

IDEX · 19-23 février 2023 · Emirats Arabes Unis

SOFINS · 28-30 mars 2023 · Souge (Bordeaux)

FIC · 5-7 avril 2023 · Lille

DEFEA · 9-11 mai 2023 · Grèce

EDEN DAY · 5 juillet 2023 · Paris

FED · 4-5 octobre 2023 · Satory (Versailles)

DSEI · 12-15 septembre 2023 · Royaume-Uni

MILIPOL · 14-17 novembre 2023 · Paris Villepinte

Ils nous ont rejoints

teXys GROUP

blockaxess la sécurité optimale

Tenexium

Journée CyberAix (Savoie)

L'IHEDN Dauphiné Savoie, la CCI Savoie et la mairie d'Aix les Bains organisent le 16 mars prochain un événement dédié à la cybersécurité, **CyberAix**. Cet événement se tiendra au palais des congrès André Grosjean d'Aix les Bains à partir de 16h00.

Ces premières rencontres visent à sensibiliser les PME et les collectivités territoriales à la menace cyber. Centrées autour de deux tables rondes (un territoire face aux enjeux cyber et quel hygiène numérique), ces rencontres se concluront par une conférence de Nicolas Arpagian, auteur notamment en 2018 du Que sais-je ? sur la cybersécurité (PUF) et de « Frontières.com » aux Éditions de l'Observatoire en 2022. A noter que Fabrice Koszyk, DG de Serenicity participera à une de ces tables rondes.

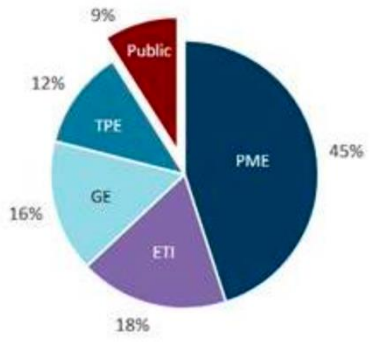
Rappelons que le Cluster EDEN est partenaire de l'association des auditeurs de l'IHEDN Dauphiné Savoie et, qu'à ce titre, notre association soutient les actions contribuant à la diffusion de l'esprit de défense et de sécurité.

Les modalités d'inscription à CyberAix seront précisées ultérieurement.

La cybersécurité : en tant que membre du Cluster EDEN, suis-je concerné ?

Le numérique occupe aujourd'hui une place prépondérante dans le fonctionnement des entreprises quelle que soit leur taille – y compris pour les plus petites d'entre elles. Cette situation suscite un intérêt toujours croissant des cybercriminels.

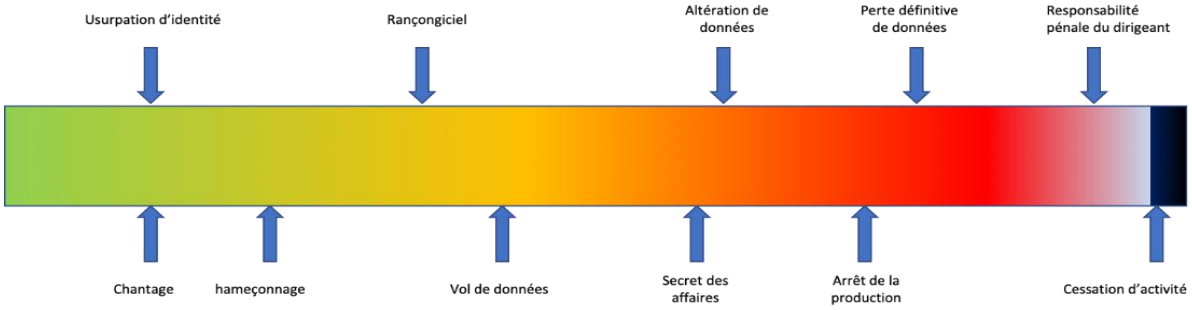
Les cyberattaques et les cyber escroqueries se sont intensifiées au fil des ans. Comme le démontre l'actualité, des grandes entreprises aux plus petites, des administrations aux collectivités locales, des hôpitaux aux particuliers en passant par des associations… Tous les acteurs de la société en sont quotidiennement victimes et peuvent en subir le préjudice.



Répartition des attaques informatiques en 2022

Mais quels sont exactement les risques pour les TPE, PME et ETI, et comment y faire face ?

La cyber sécurité peut avoir des conséquences mineures mais aussi occasionner des drames pouvant aller jusqu'à la cessation d'activité.



Les plus petites entreprises sont souvent peu conscientes des risques et ne prennent pas forcément les mesures nécessaires pour se protéger, car elles pensent souvent, à tort, que leur taille ou leur activité ne sont pas assez significatives pour intéresser des cybercriminels. En réalité, c'est tout le contraire : les cybercriminels ont bien compris que toute entreprise, quelle que soit sa taille, constitue une valeur marchande, que ce soit à travers une trésorerie potentielle ou des informations qu'elle détient. Et les petites entreprises sont d'autant plus faciles à pirater qu'elles sont souvent moins protégées. La nature des données manipulées par les entreprises du Cluster EDEN attise d'autant plus la convoitise des criminels qu'ils aient une volonté cyber à la base ou alors un objectif ciblé pour voler des informations sensibles voire classées.

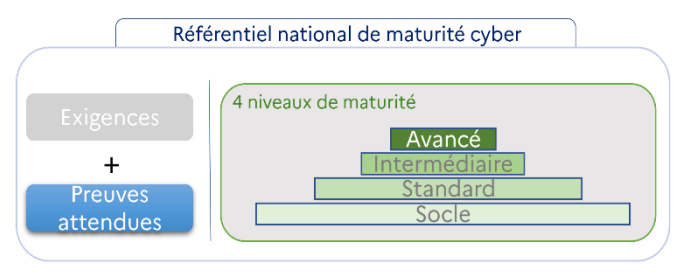
Pour une TPE ou PME, les conséquences d'une cyberattaque peuvent s'avérer très importantes et parfois même désastreuses : perte immédiate d'argent suite à une fraude au virement, perte d'exploitation ou arrêt de l'activité, suite à une attaque par rançongiciel, qui prendra en otage les données de l'entreprise contre une rançon. Toute cyberattaque a un coût direct et indirect pour l'entreprise qui en est victime. C'est évidemment le coût non planifié de remise en état du système attaqué et de reconstitution, lorsque c'est possible, des informations détruites, comme le fichier clients, les contrats, la facturation ou la comptabilité, etc. Mais c'est également un coût lié à la réputation de l'entreprise et à la perte de confiance des salariés, des clients, des fournisseurs et même des investisseurs qui peut avoir de sérieuses incidences dans la durée en termes de chiffre d'affaires ou de développement de l'entreprise. Souvent fragiles financièrement, certaines petites entreprises victimes de cyberattaques se voient contraintes de cesser leur activité. De plus, la responsabilité juridique civile et pénale du dirigeant peut même parfois être engagée en cas de manquements à ses obligations de protection de ses systèmes informatiques et des informations à caractère personnel détenues par son entreprise.

La rançon « **peut s'élever jusqu'à 128 000 € en moyenne par entreprise** », d'après le baromètre d'Anozr Way.

La DGA prépare la défense…

Afin de structurer la démarche cyber et de renforcer le niveau de sécurité de la chaîne de valeur composée par les différents acteurs de la défense, la DGA prépare **un nouveau cadre normatif** permettant d'évaluer le niveau de sécurité des acteurs.

DGA



Source DGA

Le cadre normatif sera composé de 4 niveaux.

Ce dispositif ne sera pas basé uniquement sur des exigences mais, prévoira des audits pendant lesquels des preuves de conformité devront être présentées.

Les 20 principaux types d'attaques informatiques :

1. L'arnaque au faux support technique
2. Les attaques en déni de service (DDoS)
3. Le chantage à l'ordinateur ou à la webcam prétendus piratés
4. Le cyberharcèlement ou le harcèlement en ligne
5. L'escroquerie aux faux ordres de virement (FOVI)
6. La défiguration de site internet
7. Les fausses offres d'emploi créées par des fraudeurs
8. La fuite ou violation de données personnelles
9. La fraude à la carte bancaire
10. L'hameçonnage (***phishing*** en anglais)
11. Le piratage de compte
12. Le piratage de compte de l'espace d'un recruteur
13. Le piratage d'un système informatique (particuliers)
14. Le piratage d'un système informatique (professionnels)
15. Les propositions d'emploi non sollicitées
16. Les rancongiciels (***ransomwares*** en anglais)
17. Le spam électronique
18. Le spam téléphonique
19. L'usurpation d'identité
20. Les virus informatiques

Les bonnes pratiques :

1 - Vital pour la continuité opérationnelle : avoir des sauvegardes régulières, vérifiées et mises hors ligne

2 - Indispensable pour le secret des affaires et le maintien de l'avantage concurrentiel : avoir de vrais mots de passe et idéalement une authentification multi facteurs et l'application systématique du moindre privilège.

3 - Réduire la surface d'exposition au risque : mettre à jour régulièrement tous les ordinateurs, smartphones ou serveurs. Et avoir des antivirus et ou des EDR à jour
Ne jamais installer d'application qui ne soit pas issue de magasin officiels et certifiés.

EDEN
CYBER

Dans sa feuille de route pour l'année 2023, le GT cyber se propose de publier au profit des adhérents EDEN des lettres d'informations à fréquence régulière. Dans les prochaines, vous retrouverez une présentation de ses membres, mais également des clefs pour faire face à une attaque informatique ciblée, un ransomware, une usurpation d'identité, pour se doter de dispositifs de détection de flux toxiques sur les réseaux, et nombreux autres conseils pour se protéger ensemble dans le cyber espace.

Retour en image sur les trois derniers mois

INDODEFENCE

2-5 novembre 2022 - Indonésie

ASSEMBLEE GENERALE

17 novembre 2022 - Lyon

EDEN DAY MCO

9 novembre 2022 - Paris

JOURNEES AGIR GENDARMERIE

24 novembre 2022 - Paris

DGA PME TOUR

8 décembre 2022 - Le Creusot

NOMINATION VICE-PRESIDENCE EDEN EST

Janvier 2023 - EDEN EST