NOUVELLES CYBER MENACES, COMMENT SE PREPARER ?

FCBA INFO

La question n'est pas de savoir si vous allez être attaqué, mais quand !

Voilà la question qui a ouvert la conférence Afnor du 12 janvier sur le thème des nouvelles cyber-attaques. En effet, sur les 10 derniers mois de l'année 2017, le monde a connu les 10 plus grandes cyber-attaques à ce jour avec, parfois plusieurs dizaines de milliers de pc infectés. Plus on avance, plus le risque grandit. Demain, encore plus d'objets seront connectés et seront donc des portes ouvertes pour l'intrusion d'un virus.

Le risque est tel que la réglementation exige désormais des grands opérateurs/acteurs la capacité à avoir un plan de continuité de l'activité. Imaginez la pénétration d'un virus au sein d'une centrale nucléaire ou d'un barrage ? Cependant, si l'on comprend bien qu'il existe des risques majeurs à l'échelle d'opérateur stratégique, les risques existent malheureusement aussi au niveau des PME. Que faut-il donc faire en tant que PME pour se protéger ?

Rappel du contexte

En 2016, 8 entreprises européennes sur 10 ont connu au moins une cyber-attaque. Plus de 4000 attaques par raçongiciel ont eu lieu chaque jour en Europe, ce qui correspond à une augmentation de 300 % par rapport à l'année précédente. **La cybercriminalité est belle et bien en hausse.**

Plus d'un quart des PME françaises auraient été victimes de cyber malveillance en 2016, mais à peine 5 % d'entre elles seraient assurées contre ces risques, alors qu'une entreprise sur deux ne possède pas de solution de cyber-sécurité. Associer la cybercriminalité industrielle uniquement aux grands groupes et attaques de grande ampleur, **c'est donc oublier que ce sont les PME qui représentent 99,8 % des entreprises en France et sont les principales victimes de la cybercriminalité**

C'est donc face à ce contexte que de nombreux acteurs se mobilisent. **Afnor a sorti un guide** BP Z 90-001**.** L'objectif est de présenter une méthodologie d'approche, de détection et de traitement pour accompagner les organisations dans la prévention et la gestion des nouvelles menaces. La compagnie régionale des commissaires aux comptes a également publié un livre blanc sur la cybercriminalité.

Enfin à côté de ces documents, les centres techniques industriels dont FCBA ont également élaboré un guide gratuit à la destination des PME de leurs secteurs industriels avec des fiches méthodologiques simples. L'objectif de cet article est de vous en présenter le contenu rapidement.

Quelles sont les motivations des menaces ?

La première motivation peut être le phénomène d'influence et cela dépasse parfois les organisations pour aller au plus haut niveau politique, c'est l'exemple du macron leaks, dont vous pourrez encore trouver tous les éléments sur le net. **La deuxième raison peut être l'espionnage industriel**. Il faut savoir que la France est le pays le plus touché dans le monde à ce sujet.

Enfin, viennent les gains financiers. C'est cependant le risque le plus fréquent au niveau des PME. En effet, non seulement, il est possible que les cyber-criminels réclament une « rançon » pour libérer les réseaux d'une entreprise, mais à ce coût direct doit être rajouté le coût d'arrêt de production, voir les augmentations des polices d'assurances…

Quels sont les impacts directs ou indirects d'une attaque ?

Les impacts peuvent être volontaires ou volontaires retardés.

Les impacts immédiats sont souvent **l'arrêt de l'activité**. L'exemple s'est produit dans un hôpital où l'usage des appareils IRM était impossible par exemple. Le deuxième impact peut être la fuite d'information. Et là, il ne faut pas s'y tromper, souvent il y a un intérêt retardé. Derrière certains scandales, les dirigeants des sociétés sont « remplacés. Nous pouvons nous poser la question de l'intérêt réél de l'attaque, obtenir de l'information ou faire changer la gouvernance d'une organisation ?

A l'échelle d'une PME, une fois encore les impacts directs sont financiers, et indirectement la perte de confiance que des tiers (clients ou fournisseurs) peut accorder à cette entreprise. Pour prendre un exemple concret, une pme a été attaquée un 16 juillet par un virus qui a eu la capacité à aller dans la directory des dossiers fournisseurs de la comptabilité. Il a changé tous les RIB des fournisseurs pour un autre RIB. L'entreprise recevant une facture versait donc directement sur un faux compte les montants réclamés par ses fournisseurs… il a fallu six semaines et quelques dizaines de milliers d'euros plus tard pour que l'entreprise se rende compte de la malveillance. Non seulement l'entreprise a perdu plusieurs dizaine de milliers d'Euros, mais elle a aussi perdu la confiance de ces fournisseurs qui ont mis un temps très conséquent à obtenir le paiement réél !

Quels sont les principaux vecteurs et tendances ?

Les logiciels de rançonware sont bien connus. Mais nous faisons face à des systèmes de fishing ou hameçonnage qui sont de plus en plus sophistiqué car l'attaque est de mieux en mieux préparé en amont. Enfin l'attaque peut se faire par des outils tiers (système de mise à jour). **Cependant, encore aujourd'hui 90% des attaques font leur entrées par des emails et notamment des url ou pièces jointes. D'où l'importance de la sensibilisation des collaborateurs. L'un des enjeux mis en avant par le guide inter-cti.** Nous y reviendrons ci-dessous.

Quels sont les enjeux pour les PME ?

Au-delà des définitions, **le guide rédigé par les cti définit six enjeux majeurs pour les PME**.

Il a été écrit à la **destination des dirigeants de PME pour les sensibiliser aux enjeux importants**. Il est consensuel puisqu'écrit avec la vision des plusieurs filière (pas de vision dédiée filere bois / Beton ….). L'approfondissement des thèmes est possible par les références insérer dans les fiches.

La PME ciblée sera donc de petite taille sans forcément de DSI ou Service informatique.

Il présente aussi rapidement la responsabilité des PME et bien sûr des sources d'informations fiables.

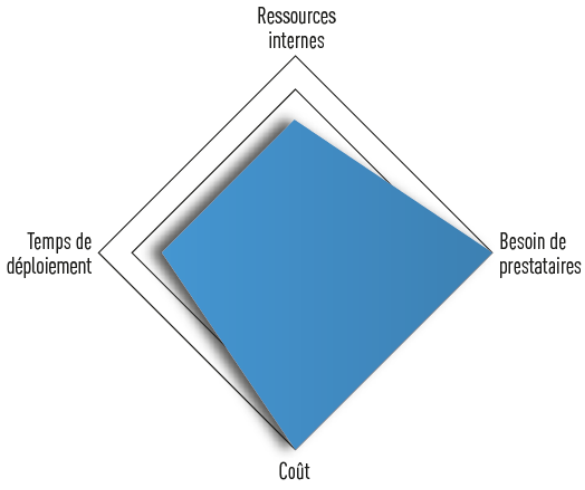
Chacun des enjeux y est traité sous forme de fiches pratiques qui permet au chef d'entreprise ou au collaborateur en charge de l'action d'identifier les risques, de trouver des recommandation et d'évaluer la facilité de mise en œuvre au sein de l'organisation.

Les six enjeux majeurs identifiés sont

- ✓ Sensibiliser guider et former les collaborateurs (6 fiches)
- ✓ Garantir le fonctionnement de l'atelier/outil de production (4 fiches)
- ✓ Protéger ses données et son patrimoine immatériel (2 fiches)
- ✓ Sécuriser la relation avec fournisseurs et sous-traitants (1 fiche)
- ✓ Sécuriser la relation avec ses clients (2 fiches)
- ✓ Fournir des produits connectés et/ou services associés sécurisés (1 fiche)

Enfin pour chacune des fiches, vous trouverez une liste de sources d'information et un indicateur de facilité de mise en œuvre des actions.

Facilité de mise en œuvre



ENJEU N°1 PAGE
Sensibiliser, former et guider les collaborateurs

1. Sensibiliser ses collaborateurs 17
2. Utiliser des outils nomades, ... 19 accès à distance
3. Communiquer via les réseaux ..... 21 sociaux,messagerie, internet
4. Briser les frontières entre les ..... 23 différents services (notamment entre les systèmes informatiques et les systèmes industriels

ENJEU N°2
Garantir le fonctionnement de l'atelier et de l'outil de production

5. Garantir le fonctionnement ..... 25 des machines
6. Contrôler les accès 27
7. Maîtriser la gestion et l'échange ..... 29 des données numériques internes
8. Assurer la traçabilité de ..... 31 la production

ENJEU N°3
Protéger ses données d'entreprise, son patrimoine immatériel

9. Sauvegarder et protéger ..... 33 les données et logiciels
10. Services en ligne et Cloud 35

ENJEU N°4
Sécuriser la relation avec les fournisseurs et sous-traitants

11. Sécuriser les données ..... 37 numériques avec l'extérieur

ENJEU N°5
Sécuriser les échanges contractuels et financiers relatifs aux ventes

12. Sécuriser les documents officiels .... 39 et engagements contractuels
13. Maîtriser les flux financiers et ..... 41 commandes dématérialisées

ENJEU N°6
Fournir des produits connectés et/ou services connectés sécurisés

14. Sécuriser les produits et ..... 43 services connectés

Et si malheureusement l'attaque a eu lieu, que faire ?

Si les phases de prévention et détection ont été défaillante, malheureusement, c'est donc « au traitement » qu'il faut avoir recours.

Bien évidemment la priorité doit être donnée au retour en fonctionnement de l'entreprise mais ensuite il peut être utile ou intéressant d'entamer une action civile ou pénale. L'action pénale peut avoir un intérêt dans certains cas si on espère avoir réparation. Lorsque l'on veut plus simplement faire reconnaitre un préjudice, souvent, c'est plus une action civile.

A noter qu'à partir du mois de mai 2018, il y aura une obligation déclarative d'une cyber-attaque.

Dès lors que l'on va vouloir faire reconnaître un préjudice, il va falloir faire évaluer l'ampleur réelle du problème, il faut donc mener une cyber investigation. Il existe des experts agréés pour faire ces enquêtes car le DSI n'a pas le droit d'enquêter. Les experts agréés appartiennent au CNAPS. Le rapport d'enquête numérique qui est fait permet de calculer le préjudice et d'obtenir un remboursement à condition de s'adresser directement au procureur de la république.

Quid vis-à-vis des assurances ?

A ce jour, le risque de cyber attaque n'est pas toujours mis en avant dans les contrats d'assurance, on peut donc parfois considérer qu'il est couvert par défaut. Cependant, les assureurs prennent de plus en plus conscience du risque, et il n'est pas rare que lors d'un renouvellement de la police d'assurance de l'entreprise, soit insérer de nouvelles conditions ou clauses pour couvrir ce risque. Evidemment qui dit nouveau risque dit nouveau coûts pour la protection…

Pour obtenir le guide

Ce guide est gratuit, en téléchargement ici.

> le nouveau guide publié par le réseau des centres techniques industriels

Contact

Valérie GOURVES ● valerie.gourves
Tél. 01 72 84 97 30

FCBA
INSTITUT TECHNOLOGIQUE

Pôle Ameublement
Direction du pôle
10 rue Galilée, 77420 Champs-sur-Marne