Sécurité informatique

Jean-Etienne Fortier

(Oct 2023)

IPSO MEDIC MEL
Aubagne

Quel enjeu pour IPSOMEDIC / IPSOMEL ?

- Aujourd'hui l'informatique simplifie et relie toutes les fonctions dans une entreprise. Les réseaux relient les employés et leurs données entre eux.

- Dans la recherche, les études et données produites sont des cibles pour les attaquants, y voyant un moyen de sabotter l'entreprise, l'espionner ou bien se faire de l'argent.

Vulnérabilités informatiques

Une vulnérabilité est une faille majeure dans un système informatique. Elle permet à un attaquant externe de d'accéder à l'intégrité du réseau d'information.

Une attaque sur un système peut ensuite se propager sur chaque appareil de chaque utilisateur de ce dernier.

Un seul appareil infecté peut se répandre à l'ensemble du réseau.

Profil des attaquants

- Il existe aujourd'hui une grande variété d'attaquants, les plus présents aujourd'hui et qui menacent les entreprises sont majoritairement :
    - Des **hacktivistes** motivés à des fins politiques, souhaitent principalement faire passer un message.
    - Des **cybers terroristes**, souhaitent causer la peur et des dommages.
    - Des **cybercriminels** plus généralistes, faisant des espionnages et attaques, à leur compte ou à celui d'un état.

- Pour ces différents profils d'attaquants, une entreprise dans le domaine médical a plus de chances d'être prise pour cible. Cette entreprise peut représenter beaucoup d'argent, de par leurs recherches et brevets, elle peut aussi être reliée à un état ou à une institution, et peut également offenser des attaquants vis-à-vis de leurs croyances.
- De plus, les attaquants s'en prennent surtout aux **PME**, qui sont souvent mal protégées.

Les 2 causes

- 2 causes : vulnérabilités matérielles et humaines

Le PC d'un employé est protégé par un anti-virus et **surtout** par les bons comportements de son utilisateur.

Le réseau et les serveurs de l'entreprise sont protégés par un pare-feu.

Les cloud (notamment Microsoft) sont ultra protégés, et il est compliqué d'attaquer une entreprise depuis ce dernier. L'entreprise ne peut pas agir sur la sécurité du cloud.

C'est l'**option privilégiée** par IPSOMEDIC et IPSOMEL pour stocker nos données clés.

Intrusion d'un attaquant

Employé sur son PC

Reçoit un email avec un lien ou une pièce jointe (comportant un virus)

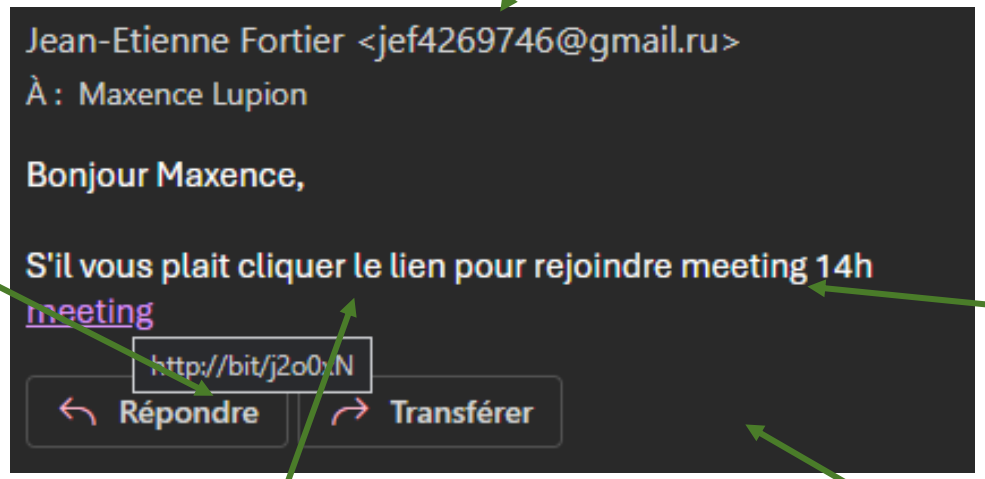
Télécharge un logiciel sur un site mal contrôlé (comprenant un virus)

Reçoit un message demandant ses identifiants (pishing et usurpation d'indentité)

L'attaquant pénètre sur son PC, et peut l'attaquer comme il le souhaite: chiffrement de données, vol de données (espionnage), suppression des données,...

Exemple d'attaque

Nom déformé, structure d'email étrange.
Evitez les emails dont vous ne connaissez pas l'expéditeur



Le lien me parait étrange, je ne devrais pas cliquer dessus.
En passant la souris, sans cliquer, je peux voir la vraie destination du lien.

Le message reste très vague.: la raison de la réunion n'est pas expliquée,

Présence de faute d'orthographe, mauvaises traductions ou de mot clés séparés par des espaces

Il semble manquer des informations sur l'expéditeur, pas de signature ?

Plusieurs réflexions doivent arriver:

- Si cette personne appartient à mon organisation, pourquoi ne pas m'avoir informé par Teams ?
- Est-ce que je connais cet expéditeur ?
- Pourquoi m'inciter à accéder à un lien/télécharger un document (pièce jointe) ?

Example d'attaques

- Fin mars 2021, le groupe pharmaceutique *Pierre Fabre* est victime d'un ransomware demandant 25 millions de dollars. La rançon n'a pas été payée et l'entreprise a du s'adapter pour suivre leur production et la disponibilité de leurs produits.

- En 2017, la PME *Clermont pièces* est victime d'une attaque qui va supprimer ses données. Elle ne pourra pas suivre ses commandes ni sa production, et mettra la clé sous la portes quelques mois plus tard.

Comment l'entreprise nous protège ?

Logiciel Vade : Protège les boites mails en détectant les attaques

Antivirus ESET : Protège les ordinateurs individuels (installation de virus, hameçonnage, etc.)

Pare feu installé sur le réseau : Protège le réseau interne d'une attaque extérieure

2 réseaux wifi (Ipsomedic / Ipso guest): protège d'une attaque de l'intérieur

Un seul responsable système

Une stratégie cloud (OndeDrive, SharePoint, SILAE RH, etc.)

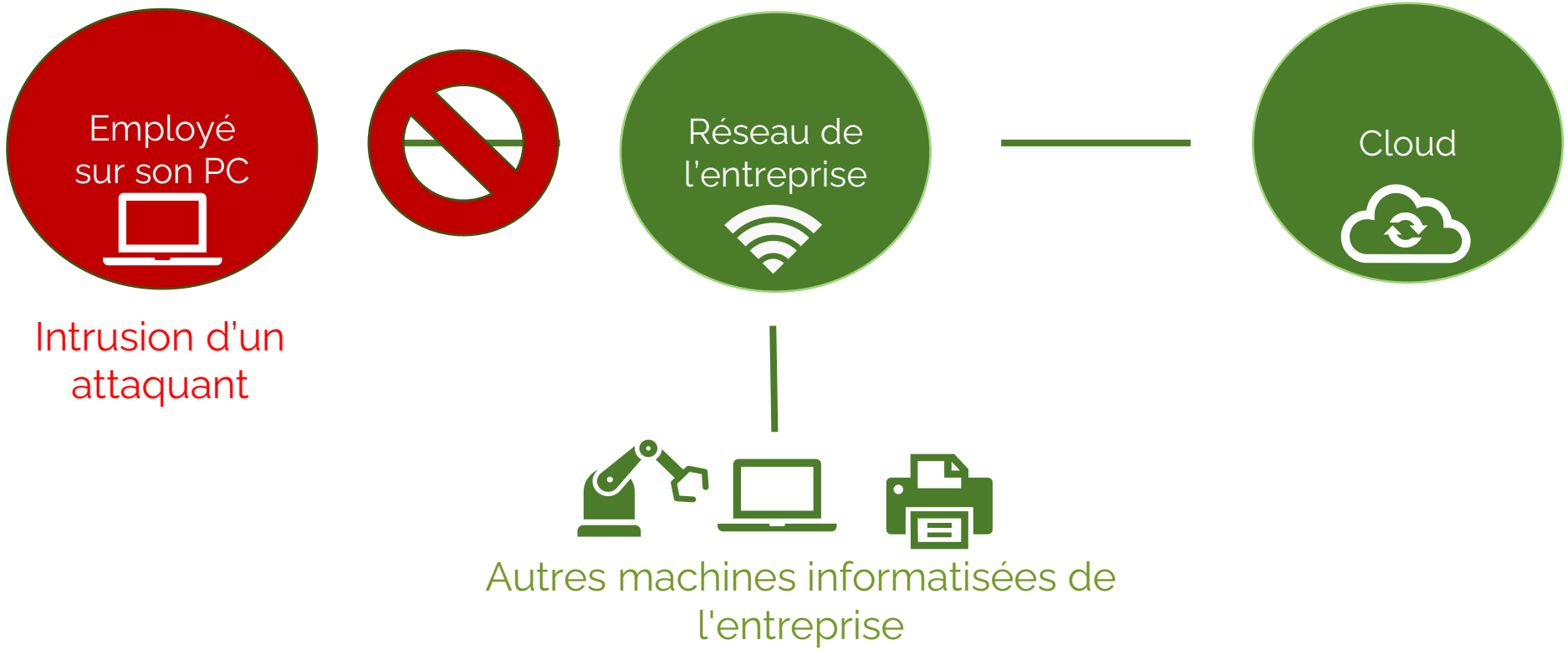
La généralisation de la double authentification

10 règles d'or

1. Utilisation de mots de passe solide. > 12 caractères, majuscule, minuscule, chiffre et caractère spécial. => 226 ans
Ce mot de passe ne doit rien dire sur vous. De plus, il est conseillé de diversifier ses mots de passe sur les services et les changer régulièrement.
2. Ne jamais laisser son ordinateur déverrouillé en son absence. **Windows L** pour verrouiller sa session.
3. Appliquer les mises à jour de sécurité sur ses appareils et logiciels.
4. Faire attention lors de téléchargement. En cas de doute, ne prenez pas le risque d'y télécharger quoi que ce soit, ou demandez une confirmation.
5. Faire attention aux messages/emails reçus. Si un message louche est reçu d'un émetteur connu, allez directement lui demander.
6. Ne pas se connecter aux réseaux wifi public. En extérieur vous pouvez utiliser votre téléphone pour faire modem (partage de connexion). Le wifi de votre téléphone doit contenir un mot de passe solide
7. Ne jamais connecter de périphériques d'origine externe à son ordinateur (disque dur, clé USB, etc.), y compris les périphériques personnels.
8. Ne stocker des données que sur le cloud Microsoft proposé par IPSOMEDIC, et non localement.
9. Ne **jamais** partager ses identifiants, peu importe l'interlocuteur (famille, manager, collègues, banquier). **Personne** n'est censée vous les demander et vous ne devez jamais les divulguer.
10. Prendre soin de ses informations pro et perso, et de son identité numérique. On ne doit pas savoir qui vous êtes, ni qui vous fréquentez à travers vos actions sur internet.

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years

En cas d'attaque sur un PC



- **Réaction de l'employé / entreprise: déconnexion du réseau wifi depuis l'appareil attaqué, afin de limiter sa propagation.**

En cas d'incident

Si malgré les mesures mises en place, et qu'un attaquant a pénétré le système, l'ANSSI nous recommande ceci :

- En cas de comportement inhabituel de votre ordinateur, vous pouvez soupçonner une intrusion
  - impossibilité de se connecter,
  - activité importante
  - connexions ou activités inhabituelles
  - fichiers créés, modifiés ou supprimés sans autorisation
- Déconnecter la machine du réseau wifi de l'entreprise

- Prévenir sa hiérarchie par **TELEPHONE** ou de **VIVE VOIX**
- Faites faire une copie physique du disque (rien ne devrait s'y trouver)
- Après l'incident, changez l'intégralité de vos mots de passe

Questions ?

IPSO MEDIC MEL
Aubagne