Pôle Activ'Océan
9 Rue de Bois Fossé
85300 CHALLANS
Tél. 02 51 49 31 31

espace technologie

FICHE CONSEIL

La protection avancée de votre Système d'Informations

Table des matières

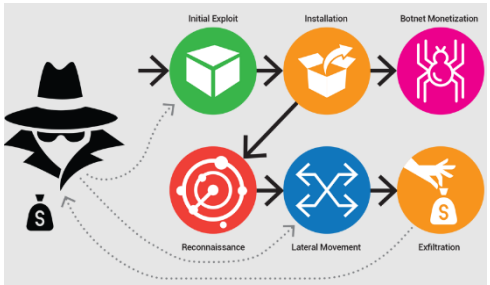
❖ Introduction

Ce document est un retour d'expérience par suite de différents audits d'intrusion de notre expert en Cyber Sécurité.

Nous constatons que de nombreux responsables considèrent qu'il suffit d'être équipé d'un bon antivirus et d'un firewall pour être protégé contre les cyber-risques. Ce n'est plus vrai.

L'objectif de ce document est de vous faire comprendre que désormais ces outils sont indispensables mais loin d'être suffisants.
En effet, les sécurités périmétriques sont très satisfaisantes mais sont inopérantes pour contrer les actions malveillantes menées par des personnes hostiles au travers du réseau ayant réussi à usurper une identité.

❖ Rappel de la killchain



Définition : La KillChain est le nom « barbare » utilisé par les spécialistes de la sécurité informatique pour définir les processus utilisés par les cybercriminels pour lancer une attaque destructrice. Les attaquants procèdent toujours de la même manière, celle référencée ci-dessous :

Les 7 phases de la KillChain :

- Reconnaissance
- Intrusion initiale dans le réseau
- Établissement d'une porte dérobée dans le réseau
- Obtention d'identifiants d'utilisateurs

- Installation de programmes utilitaires malveillants divers
- Élévation des privilèges* / mouvement latéral / exfiltration de données
- Maintien dans le système cible

* Privilèges : Droits d'accès utilisateurs sur le réseau. Le but est d'obtenir les privilèges de comptes afin d'obtenir tous les droits de modification/exfiltration/destruction/chiffrement des données.

Le rôle de l'antivirus.

L'antivirus joue un rôle de protection des postes de travail et des serveurs contre les virus.

L'antivirus sera inefficace si l'attaquant a déjà obtenu les droits d'un compte utilisateur.

Il est désormais habituel que des attaquants restent des jours, des semaines voire des mois, infiltrés dans le système d'informations. Le but est de collecter un maximum d'identifiants, afin d'effectuer une élévation de privilège (un compte administrateur étant un objectif) ainsi que de pouvoir rebondir sur les systèmes de sauvegardes et hyperviseurs.

Un attaquant compétent, ayant usurpé un compte utilisateur, sera en mesure de reconnaitre l'antivirus en place, de le contourner et de le rendre inopérant, sans que l'utilisateur propriétaire du compte ne s'en rende compte. **A ce stade, le système d'informations est en DANGER.**

❖ Le principe de la furtivité

Lors d'un audit Cyber, notre expert suivra les mêmes étapes que celles de la killchain.
Son objectif premier sera de récupérer un premier compte utilisateur sur le système d'informations en utilisant les mêmes méthodes que les cybercriminels.

1- L'expert commencera par découvrir l'environnement dans lequel il évolue.

A ce niveau, l'antivirus ne détecte rien car l'expert interroge les services légitimes du réseau (DNS, IP, etc…)
C'est le firewall qui, potentiellement, devrait détecter et bloquer l'intrus. Malheureusement, un firewall n'a pas les capacités et l'intelligence de détecter si la requête est légitime ou non. En effet, le Firewall est positionné en entrée/sortie du réseau (Nord/Sud) mais ne surveille pas les interrogations latérales du réseau (Est/Ouest).

2- Ensuite notre expert va se mettre en position « d'homme du milieu » et tenter de collecter des mots de passe chiffrés qui circulent sur le réseau ou (plus facile) rechercher des comptes génériques mal protégés.

Les antivirus sont inopérants car tout se passe à l'intérieur du réseau.
Il est très difficile de détecter une attaque dite « Homme du milieu », mais cependant pas impossible.

3- Une fois en possession d'un compte utilisateur, l'expert va pouvoir se connecter aux ressources de l'entreprise et rechercher des fichiers de configuration /script ou toutes autres informations utiles, afin d'escalader les privilèges à la recherche de comptes avec plus de pouvoir.

Encore une fois, l'antivirus ne donnera pas l'alerte car ces recherches peuvent être légitimes voire obfusquées.

4- Enfin, en possession d'un compte à pouvoirs, il va être facile de rechercher des ressources essentielles du système d'informations afin de compromettre les sauvegardes et les serveurs sur site ou dans le cloud.

5- A ce niveau, un cyber criminel activera un rançongiciel (modifié spécialement pour que l'antivirus ne le détecte pas). Le pirate aura tout loisir de chiffrer le système d'informations, les sauvegardes ainsi que les données éventuelles stockées dans le Cloud. C'est à ce moment que le pirate demandera une rançon en échange d'une hypothétique clé de décryptage.

Sans la clé de décryptage toutes les données seront irrémédiablement perdues et le S.I. à l'arrêt.

Comment contrer ce type d'attaque très courante depuis 1 ou 2 ans?

L'attaquant a pour objectif d'être le plus furtif possible afin de ne pas être détecté.
Nous allons donc appliquer la même méthodologie. (Espionnage/Contre-Espionnage !!).
Nous allons mettre en place un équipement en mode furtif particulièrement redoutable.
Cet équipement (Appliance) sera connecté à l'un des switches du réseau dans le but de surveiller tous les échanges qui circulent entre les machines/serveurs et autres équipements informatiques.
Cet équipement furtif embarque une intelligence artificielle permettant de lancer une alerte dès qu'une opération inhabituelle ou critique se produit sur le réseau.
L'attaquant, bien entendu, ne pourra pas le détecter.
Nous avons également la possibilité de mettre en place un « pot de miel ».
Un pot de miel est un ordinateur du réseau qui doit immédiatement intéresser l'attaquant. Cette machine présentera de « fausses » vulnérabilités et un compte facilement prédictible (compte par défaut par exemple). Lorsque l'attaquant essayera de prendre le contrôle de cet équipement, nous serons immédiatement informés « priorité haute » et serons en mesure de détecter l'attaquant à coup sûr.

Il est extrêmement important de ne donner aucune indication à l'attaquant, par conséquent aucun agent n'est installé sur les postes utilisateurs et serveurs, contrairement aux solutions antivirus.
Si un attaquant usurpe un compte utilisateur, il se connectera à une ressource et fera un état des lieux précis des programmes s'exécutant sur l'équipement. Notamment les politiques de sécurité en place, les antivirus.
L'I.A. embarquée nous préviendra immédiatement de cette action inhabituelle.

❖ Les NDR

Vous venez de comprendre (je l'espère) le fonctionnement de ce que l'on appelle le « NDR » (network detection and response).
La solution NDR interagit avec les équipements périmétriques, (antivirus, firewall, log du contrôleur de domaine, accès à la base des comptes AD, etc…) afin de bloquer immédiatement la machine ou le compte suspect.
Le NDR dernière technologie implémente le mode apprentissage et l'intelligence artificielle.

❖ Et les Firewall dans tout ça ?

Les firewalls ont deux rôles principaux :

- Protection des entrées/sorties du réseau vers l'extérieur (Nord/Sud).
- Isoler différentes zones du réseau (sous réserve que le réseau ait été préalablement segmenté).

Le Firewall est indispensable pour se protéger des attaques extérieures. Mais il est incapable (la plupart du temps) d'analyser le réseau interne.
Si l'attaquant est déjà présent à l'intérieur du réseau après avoir usurpé un compte utilisateur, il devient extrêmement compliqué voire impossible pour le firewall de détecter les actions illégitimes et malveillantes.
De plus, il n'y a pas de corrélations d'alerte et l'analyse des logs peut être fastidieuse et chronophage.

Il faut désormais considérer qu'un firewall est indispensable mais insuffisant, au même titre que l'antivirus.
Un attaquant infiltré dans le système d'informations ne rencontrera aucune difficulté à détecter le type de firewall en place et pourra adapter son attaque en fonction des caractéristiques de celui-ci.
Le NDR, quant à lui, sera invisible pour le cyber criminel ou le collaborateur malveillant.

❖ Quelles solutions adopter en fonction des coûts et de l'analyse technique

Malheureusement, les solutions NDR du marché sont onéreuses et nécessitent une ressource humaine spécialisée en interne afin d'analyser les alertes et les flux.
Aucune solution du marché n'était jusqu'à présent adaptée au budget des petites et moyennes entreprises.

Nos équipes cyber et développement ont travaillé afin de mettre au point une solution NDR qui n'a rien à envier aux solutions du marché haut de gamme.
La différence se situe au niveau du prix de la solution et de la supervision humaine des alertes.
Notre solution « NDR-ET » est disponible à un prix raisonnable pour n'importe quelle TPE et inclut la supervision de la solution par nos services.
En effet, non seulement nous avons développé la solution mais nous avons mis en place une équipe de surveillance directement connectée à votre NDR.
Notre équipe est prête à intervenir à la moindre alerte suspecte vous dispensant d'embaucher un spécialiste en interne.

Pour bien comprendre l'importance du NDR, considérez le fait que 99 % des cyberattaques traversent le réseau d'une manière ou d'une autre.

Les réseaux ne mentent pas. Les données réseau capturées dans le cadre des connexions entre les appareils et les systèmes ne peuvent pas être désactivées par les attaquants comme peuvent l'être les antivirus et autres protections logicielles.

Par conséquent, toute société cherchant à améliorer sa détection globale des menaces et sa réponse aux incidents doit considérer le NDR comme un élément central de sa stratégie.

Pôle Activ'Océan
9 Rue de Bois Fossé - BP 147
85301 CHALLANS Cedex

Tél. : 02 51 49 31 31
Email : contact@espace-technologie.com
Web : www.espace-technologie.com

Organisme de formation n° 52850059385 - SAS au capital de 38 500 € - Siret : 38979357100024 - APE : 4741Z - RCS La Roche sur Yon B389793571