Parc d'Activités Schweitzer
26 rue du bois Fossé
85300 CHALLANS
Tél. 02 51 49 31 31

espace technologie

FICHE CONSEIL

STRATEGIE DE CYBER DEFENSE

NDR
NETWORK DETECTION & REPONSE

❖ Table des matières

❖ Introduction

Ce document est un retour d'expérience des différents audits d'intrusion et analyses après sinistre de notre expert en Cyber Sécurité depuis le début d'année 2022.

Nous constatons que de nombreux responsables considèrent encore, à tort, qu'il suffit d'être équipé d'un bon antivirus et d'un firewall pour être protégé contre les cybers risques.

L'objectif de ce document est d'expliquer pourquoi ces outils sont indispensables mais loin d'être suffisants.

❖ 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 cybers Criminels pour lancer une attaque destructrice.

Les 7 phases de la KillChain :

- Reconnaissance de la future victime
- Intrusion initiale dans le réseau
- Établissement d'une porte dérobée dans le réseau
- Obtention d'identifiants utilisateurs
- Installation de programmes utilitaires malveillants divers
- Élévation des privilèges* / mouvement latéral / exfiltration de données
- Veille furtive dans le système cible avant lancement de l'attaque

* Privilèges : Droits d'accès utilisateurs sur le réseau. Le but est d'obtenir les privilèges administrateurs pour avoir tous les privilèges de destruction des données.

<u>Le rôle de l'antivirus.</u>

L'antivirus à 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 mois entiers présents dans le système d'information. Le but est de collecter un maximum d'identifiants, afin d'effectuer une élévation de privilège (un compte administrateur étant le graal)

Un attaquant compétent, avec un compte utilisateur sera en mesure de connaitre l'antivirus en place et de le contourner, voire de le rendre inopérant, sans que l'utilisateur propriétaire du compte ne s'en rende compte.

❖ Le principe de la furtivité

Lors d'un audit, notre expert utilise les mêmes étapes de la killchain afin de tester les vulnérabilités du système d'information, l'objectif premier est de récupérer un premier compte utilisateur.

1- L'expert commence par prendre connaissance de l'environnement dans lequel il évolue.

A ce niveau, l'antivirus ne détecte pas l'intrus car il interroge les services légitimes du réseau (DNS, IP, etc…)
C'est le firewall qui devrait détecter et bloquer. Mais un firewall n'est pas en mesure de savoir si les requêtes sont légitimes ou non ?

2- Ensuite notre expert va se mettre en position « d'homme du milieu » et essayer de collecter des mots de passe chiffrer qui circule sur le réseau ou rechercher des comptes génériques mal protégés.

Là encore les antivirus sont inopérants car tout se passe dans le réseau local.
Dans le cas d'un « homme du milieu », il est très difficile de détecter cette attaque.
Dans le cadre d'un test de couple utilisateur générique/mot de passe fragile, les antivirus ont la plus grande peine à détecter une attaque par brute force*.
** Brute Force : L'attaque par force brute est une méthode simple, utilisée en cryptanalyse pour trouver un mot de passe ou une clé. Il s'agit de tester, une à une, toutes les combinaisons possibles*.

3- Une fois en possession d'un compte utilisateur, l'expert pourra se connecter aux ressources de l'entreprise et rechercher de fichiers de configuration /script ou tout autres informations utiles, afin d'escalader les privilèges à la recherche de compte avec plus de pouvoir.
4- Enfin, en possession d'un compte à pouvoir, il sera possible pour un pirate de rechercher des ressources essentielles du système d'information afin de compromettre les sauvegardes et les serveurs sur site ou dans le cloud.
5- A ce niveau, un cyber criminel activera un rançon logiciel modifier spécialement pour que l'antivirus ne le détecte pas. Désormais tout le S.I. est chiffré et sans la clé de décryptage toutes les données sont perdues et le S.I. est inopérant.

Comment faire dans ce cas ?

L'objectif de l'attaquant est d'être le plus furtif possible afin de ne pas être détecté.

Nous allons donc appliquer la même méthodologie pour vous défendre.

En effet, la mise en place d'un équipement en mode furtif est redoutable.
Cet équipement est installé sur un des switches du réseau et surveille tous les échanges qui circulent entre les machines/serveur et autres équipements informatiques.
Cet équipement furtif est équipé d'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 une machine qui doit immédiatement intéresser l'attaquant. Cette machine doit présenter de « fausses » vulnérabilités et compte facilement prédictible (compte par défaut par exemple). Lorsque l'attaquant essayera de prendre le control de cet équipement, nous serons immédiatement informé « priorité haute » et serons en mesure de confiner l'attaquant.

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. Ainsi, 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 le fonctionnement du NDR (network détection & réponse).
Celui-ci peut interagir avec les équipements périmétriques, antivirus, firewall, log du contrôleur de domaine, accès à la base des comptes AD, etc…) afin de bloquer immédiatement le compte ou la machine posant problème.
De plus aujourd'hui le NDR implémente le mode apprentissage et l'intelligence artificielle.

❖ Et les firewalls dans tout ça ?

Les firewalls ont un rôle de protection des entrées/sorties du réseau vers l'extérieur ou pour isoler différentes zones du réseau.
Ils sont indispensables pour se protéger des attaques extérieures. Certains firewalls sont d'excellente qualité. Mais ils sont incapables (la plupart du temps) d'analyser le réseau interne.
Si l'attaquant est déjà dans le réseau à travers un compte utilisateur, cela devient extrêmement compliqué voire impossible pour le firewall de détecter les actions illégitimes.
De plus, il n'y a pas de corrélations d'alerte et l'analyse des logs peut être fastidieux et chronophage.
Il faut désormais considérer qu'un firewall est obligatoire mais insuffisant, au même titre que l'antivirus.
Un attaquant sur le réseau aura sans difficulté l'information sur le type de firewall en place dans et pourra adapter son attaque en fonction. Un des points forts du NDR, c'est qu'il reste invisible.

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

En 10 ans, nos habitudes de travail ont changé.
Beaucoup de tâches s'effectuent dans le cloud.

- Mettre en place un NDR piloté par un analyste représente un cout de fonctionnement très important (amortissement de l'équipement, salaire de l'analyste) souvent incompatible avec les budgets des Tpes/pmes
- Il est préférable de faire confiance à une équipe d'experts mutualisés au sein d'un SOC (Security Opération Center).
  Ainsi les couts sont mutualisés.

- Espace Technologie a mis en place une solution NDR mutualisée pilotée par nos équipes d'experts. Cette solution adaptée aux TPE/PME permet de se protéger efficacement pour un budget raisonnable.

❖ Comment réagir le plus rapidement possible en limitant les coups d'analyse

Notre équipe sera réactive dès qu'un indice de compromission sera détecté.

❖ Note importante sur les bonnes pratiques

Une bonne hygiène informatique est importante.
L'ANSSI regroupe un ensemble de règles de bonne conduite afin de limiter au maximum les risques.
Nous consulter, si vous souhaitez être accompagnés dans la mise en place de ces mesures.
Nous analyserons de manière précise votre écosystème et mettrons en place, avec vous, les actions à mener à court, moyen et long terme afin de vous éviter une attaque fatale.

Parc d'activité Schweitzer
26 rue du 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