DE LA RECHERCHE À L'INDUSTRIE

Surveillance et gestion d'incidents

1

Evaluation de la sécurité

Commissariat à l'Énergie Atomique et
aux Énergies Alternatives

Février 2020

www.cea.fr

Sommaire

Sommaire

De la protection à la surveillance

- Tout commence par une évaluation des menaces (politique de sécurité) ;
  - Définir un socle de sécurité commun ;
  - Identifier les ressources critiques (systèmes, données) ;
- La protection a pour objectif d'empêcher la réalisation des menaces (sécurité des systèmes et des réseaux) ;
- La protection ne peut pas empêcher toutes les menaces :
  - Attaques inconnues ;
  - Attaques pour lesquelles il n'y a pas de correction ou de protection ;
  - Défaillances des mécanismes de protection toujours possibles ;
- La surveillance vient en complément de la protection pour identifier des cas de réalisations des menaces $\longrightarrow$ *intrusions et compromissions*.

Cycle de gestion de la sécurité

- Préparation des moyens et des mécanismes de protection et de surveillance ;
  - $\rightarrow$ Défense en profondeur ;
- Surveillance du système d'information et analyse des incidents de sécurité ;
  - $\rightarrow$ SoC et veille technologique ;
- Confinement et éradication des intrusions, restauration de l'état sain du système d'information ;
  - $\rightarrow$ Gestion d'incidents ;
- Analyse post-incident et amélioration de la protection et de la surveillance.

Principe de défense en profondeur

- Déployer autant de niveaux de défense que possible, par exemple :
  - Filtrage réseau non seulement en périphérie, mais aussi sur les routeurs internes, sur les serveurs, sur les stations ;
  - Architectures de services multi-tiers avec authentification et filtrage entre tous les composants ;
  - Administration correcte des domaines et droits utilisateurs sur les domaines…
- La surveillance vient en renfort et en complément de la protection :
  - Détection des menaces résiduelles ;
  - Surveillance du bon fonctionnement des mécanismes de protection ;
  - Détection sur les réseaux où l'on ne peut pas appliquer de filtrage ;
- La surveillance participe à maintenir la sécurité dans le temps (maintien en conditions de sécurité).

Organiser la surveillance

SOC : Security Operations Center

- Ressources humaines réservées :
  - Equipe de surveillance ;
  - Equipe d'intervention ;
- Salle dédiée avec stations et écrans adaptés ;
- Intégration dans la configuration des serveurs et stations ;
- Architecture de taille adéquate pour le système d'information surveillé ;
- Réseau de surveillance séparé de tout autre réseau de production ou de R&D ;
- Accessible à distance pour les cas d'urgence.

Bénéfices de la supervision

- Défense en profondeur ;
- Détection d'attaques inconnues ou de nouveaux schémas d'attaque ;
- Aide à l'administration du parc : détection de comportement problématiques ou polluants ;
- Rôle statistique, mise en évidence des usages du réseau et vision des menaces courantes ;
- Information pour la hiérarchie.

Vocabulaire

- Menace : élément pouvant impacter le système d'information ;
- Evénement : toutes informations reflétant l'activité du SI (captures réseau, logs des systèmes et applications) ;
- Alerte : événement impactant potentiellement la sécurité ;
- Incident : alerte qualifiée en problème de sécurité ;
- Intrusion : menace réalisée sur le SI, demande une analyse et une résolution ;

- Types de détection : signature, comportement ;
- Faux-positif : fausse alerte levée par la surveillance ;
- Faux-négatif : incident non remonté par la surveillance ;

Importance de la veille technologique

- Techniques de cartographie ;
- Fuites d'information sur les réseaux sociaux ;
- Risques des plateformes d'analyse en ligne ;
- Techniques de social engineering à la mode ;
- Vulnérabilités, évidemment ;
- Bonnes pratiques de configuration des systèmes et applications ;
- Signaux indicateurs d'attaques imminentes ;
- Logs d'applications à repérer ;
- Plateformes d'échanges d'IOC ;
- ...

Sommaire

Déroulement d'une intrusion

- **Cartographie** de la cible : réseau, utilisateurs, admins, relations externes
- Exploitation d'une **faiblesse** au travers d'un **vecteur d'attaque** : vulnérabilité, social engineering, rebond par tierce partie de confiance
- Elargissement de la compromission aux serveurs internes (on parle aussi de **mouvement latéral**)
- **Persistance** et furtivité : backdoor, rootkit, canal caché
- Mise en oeuvre de l'**objectif de l'attaquant**

Vecteurs d'attaque

- Pièces jointes : de nombreux types peuvent héberger du contenu malveillant
  - Exécutables, bien sûr
  - Scripts (Exécution sur double-clic sous Windows)
  - Documents Office, PDF
  - Peut être compressé, auto-extractible
  - Et parfois images, vidéos et autres suivant les vulnérabilités
- Site servant du contenu malveillant, parfois à son insu
- Tous périphériques USB (cadres photos par exemple)
- Complicité interne
- Social engineering (vol de mot de passe, intrusion physique)

Faiblesses d'un système d'information

Types de faiblesses

- Exposition : services exposés, profils employés sur réseaux sociaux…
- Vulnérabilités : overflow, injection SQL, social engineering
- Erreurs de conception : absence de séparation des droits
- Erreurs de configuration : configuration faible, mot de passe par défaut…
- Erreurs de filtrage : exposition des interfaces d'admin
- Comportements dangereux : applications superflues, droits d'administration à outrance

Machines ciblées

- Serveurs exposés
- Postes utilisateurs
- Tierces parties

Compromission initiale

Exploitation d'une faiblesse suivant la maturité de la cible

- Faible maturité : mauvaise gestion des correctifs et des droits utilisateurs
  - Des outils simples voire automatiques peuvent compromettre l'intégralité de la cible
- Bonne maturité
  - Résiste aux attaques simplistes
  - Attaquant motivé, compétent, disposant de temps et d'argent
  - Exploitation de vulnérabilités inconnues
  - Contournement d'anti-virus
  - Campagnes ciblées de social engineering
  - N'exclut pas la présence de machines très vulnérables

Objectifs de l'attaquant

- Mouvement latéral : propagation dans le réseau de la cible
- Exfiltration de données
- Rebond vers d'autres entités (parfois la victime n'est pas la cible finale)
- Activité type botnet : spam, DDoS
- Rançonnage, vol de mot de passe
- Défaçage
- Destruction
- Persistance, attaque différée

Contrôle distant des machines compromises

Intégration d'une backdoor ou d'un canal de commande

- Si défaut de filtrage, connexion directe
- Ajout d'une ressource dans un service compromis (par exemple webshell)
- Connexion inversée : la cible se reconnecte à l'attaquant
- Plus subtil : P2P, IRC, HTTP(S), site tiers (twitter, pastebin...)

Furtivité de la backdoor

- Application des techniques de rootkit
- Suite à l'obtention des privilèges d'admin sur une machine
- Plusieurs niveaux de sophistication (remplacement de fichiers, drivers, hyperviseur, firmware)
- Fonctions intégrées (capture de mot de passe, carte de crédit, activité botnet)

Sommaire

Typologie des outils

- Réseau (NIDS) :
  - Capture *full frame*
  - Analyse par paquets (OSI 3/4)
  - Analyse protocolaire (OSI 5+)
  - Analyse par flux
- Système (HIDS) :
  - Analyse des fichiers (antivirus)
  - Contrôle d'intégrité
  - Heuristiques sur l'état du kernel
  - Contrôle de la configuration
  - Sandboxes
- Collecte et analyse des logs :
  - Collecteurs
  - Filtres (formatage et enrichissement)
  - Indexation
  - Stockage
  - Requêtage et visualisation

Méthodes de classification

- Analyse par signature
  - Détection « directe »
  - Patterns, valeurs particulières
  - Hashes
  - Métadonnées
  - Contournements simples : offuscation
  - Risques de faux-positifs assez faible
  - Risques de faux-négatifs élevé

- Analyse comportementale
  - Détection par observation des actions
  - Séquences de flux réseau
  - Heuristiques sur les appels systèmes
  - Contournement difficile
  - Règles complexes à produire
  - Faux positifs élevés si règles peu précises

Adéquation avec le système surveillé

- Configurer les outils de surveillance :
  - Reconnaissance des adresses IP internes et externes
  - Nettoyage des règles suivant les services à protéger
  - Heuristiques sur les traces réseau et les logs à raffiner
  - Prise en compte des pratiques d'administration

- Déployer en adéquation avec l'architecture
  - Capture aux points de passage (routeurs)
  - Capture devant les services importants
  - Adapter les transferts des informations de sécurité à la capacité des réseaux de production
  - Filtrage renforcé, diodes

Sommaire

Considérations d'architecture

Système d'information du SOC

- Indépendant du système surveillé
- Services d'authentification indépendants
- Adhérence minimum au système surveillé (mais nécessaire pour remonter les informations)
- Dimensionné à la hauteur des missions
  - Capacité de stockage pour les captures réseau, les flux, les logs, les données extraites par les analyseurs
  - Capacité de traitement pour l'indexation, les scripts d'aggrégation et corrélation
- Redondant, persistant face aux pannes et arrêts électriques

Considérations organisationnelles

- Prise en compte de la politique de sécurité
- Amélioration de la politique face aux menaces observées
- Participation à l'administration des systèmes et réseaux
  - Mise en place d'audits automatisés
  - Vérification de la bonne application de la politique
  - Gestion des mises à jour, application correctes des correctifs et contre-mesures
- Rôle statistique, inventaire des systèmes et services
- Participe à une meilleure connaissance de l'utilisation du SI

Sommaire

Les objectifs des évaluations de sécurité

- Inventaire des systèmes et services
- Contrôle des faiblesses résiduelles
- Identification de systèmes compromis
- Adéquation avec la politique de sécurité
- Surveillance des évolutions du SI

Inventaire des systèmes et services

- Point de vue différents de celui des administrateurs
- Etat réel du parc, le plus exhaustif possible
- Identification des produits et des versions
- Base de départ pour l'identification des vulnérabilités
- Confronté plus tard à la politique de sécurité

Contrôle des faiblesses résiduelles

- Versions obsolètes des systèmes et services
- Vulnérabilités connues
- Faiblesses et problèmes dans les configurations
- Recherche de détails qui sortent de l'ordinaire
- Automatisée ou assistée si besoin de creuser

Identification des systèmes compromis

- Apparition de nouveaux systèmes ou services
- Nouveaux ports ouverts sur des systèmes déjà connus
- Fichiers modifiés de façon imprévue
- Ressources ajoutées dans des services
- Ajout de comptes ou modification de groupes
- Comportements anormaux

Adéquation avec la politique de sécurité

- Vérification des filtrages réseau
- Vérification des méthodes d'authentification
- Vérification des algos de chiffrement proposés et utilisés
- Vérification des ports ouverts et services disponibles
- Vérification de la protection des données stockées
- Vérification diverses : clés USB connectées, application dans les profils utilisateurs…

Surveillance des évolutions du SI

- Ajout non plannifiés de systèmes et services
- Déploiement de versions obsolètes de logiciels
- Intégration de postes nomades
- Evolution du filtrage réseau
- Evolution des pratiques d'administration
- Intégration dans la politique de sécurité (il faut la faire vivre aussi)

Sommaire

Outils de cartographie

- Premier approche d'inventaire du SI
- Différents niveaux de cartographie intéressants : IP, ports, identification des systèmes et services
- Utilisation de moteur d'indexation pour faire ressortir les évolutions
- Attention à certains types de scans qui peuvent faire planter des systèmes ou des équipements

Outils de vérification de configuration et d'intégrité des systèmes

- Ils peuvent inventorier et vérifier tous les fichiers des machines du SI
- Ils sont généralement très intégrés à l'administration des systèmes
- Deux types de contrôle de configuration : soit plutôt orienté détection des faiblesses, soit orienté bonne application de la configuration prévue (conformité)
- Le contrôle d'intégrité peut être difficile à utiliser, préférer une utilisation bien ciblée
- Le contrôle de configuration peut donner des résultats contraires à la politique de sécurité, il faut faire le tri

Scanners de vulnérabilités

- Ils embarquent un ensemble de codes d'exploitation pour des vulnérabilités connues
- Ils testent si les vulnérabilités sont effectivement exploitables (pas seulement potentiellement présentes)
- Ils testent aussi les faiblesses de configuration connues, la présence de comptes faibles…
- Il est intéressant de bien les configurer en accord avec les systèmes et services présent sur le SI
- Il est parfois difficile de les intégrer dans l'authentification du SI
- Ils produisent des rapports directement utilisables

Les outils

- Cartographie
  - Moteurs de scan : Nmap, Masscan
  - Indexation et visualisation : IVRE
- Contrôle d'intégrité
  - AIDE, Samhain
- Contrôle de configuration
  - Lynis
  - Gestionnaire de configuration en mode audit : Puppet
- Scanners de vulnérabilités OS
  - Open source : OpenVAS, Metasploit
  - Propriétaires : Nessus, CANVAS, Qualys…
  - Orientés Web : Nikto, Grabber
  - Offre commerciale très riche

Sommaire

Audits automatisés

- Intégrer des scans et audits automatisés assure la détection des écueils les plus évidents
- Positionnement :
  - Déploiement sur une machine non filtrée, avec interfaces réseau désactivées en dehors des plages d'utilisation
  - Déploiement sur serveur avec filtrage adéquat
- Intégration :
  - Utilisation de comptes spécifiques sur les machines auditées
  - Intégration si possible dans l'authentification du SI
  - Plage horaire bien identifiée
- Tout cela concourt à une bonne traçabilité des actions d'audit automatiques

Concordance avec les objectifs de sécurité

- Configuration adéquate des outils d'audit :
- Evaluation de la criticité des faiblesses en fonctions des objectifs de la politique de sécurité :
  - Niveau de sécurité désiré
  - Ressources et information à protéger
  - Maintien de versions anciennes de logiciels pour des systèmes particuliers parfois inévitable
- Eviter l'effet « mur de texte » : présenter des rapports qui mettent l'accent sur les mesures les plus importantes

Du bon usage des pentests

Pentest = Penetration test $\longrightarrow$ test d'attaque ciblé

- Les pentests ou audits ponctuels viennent compléter les audits automatisés :
  - Test d'une configuration particulière ou d'un logiciel non couvert par les outils automatiques (souvent pour des logiciels spécifiques de l'entreprise)
  - Tests plus complets sur une partie bien définie du SI
  - Identification de particularités du SI non identifiées par les outils automatisés
- Retour vers les tests automatisés pour une meilleure adéquation avec l'état du SI
- Assurer une bonne traçabilité des actions d'audit pour ne pas rater des attaques qui auraient lieu simultanément

Questions

Des questions ?

Commissariat à l'énergie atomique et aux énergies alternatives
Centre de Bruyères-le-Châtel | 91297 Arpajon Cedex
T. +33 (0)1 69 26 40 00 | F. +33 (0)1 69 26 40 00
Établissement public à caractère industriel et commercial
RCS Paris B 775 685 019

CEA/DAM/DIF