Alpa37

TP : Gestion d'un incident de sécurité

MSSI 2018-2019 – Pilotage de la SSI

ECHEVERRIA Sébastien, BUCQUOY Mathieu, THEVENET Raphaël, MAY Nathan, CORDELOIS Jonathan

26/03/2019

Table des matières

Présentation du TP

Contexte :

Le scénario ci-dessous présente le déroulé d'une attaque informatique contre un réseau d'une entreprise industrielle de Saint Etienne, la société « 42-industrial SA » :

[27/02/2020 14:58] Signalement d'un ralentissement important sur un des systèmes industriels du site de Saint-Etienne. Les équipes IT du site ne dénotent aucun incident particulier…

[28/02/2020 10:23] Signalement par un partenaire de confiance d'un fichier PE « dem352.exe » ainsi que d'un condensat cryptographique SHA-1 «f161ebd29699d93411cec0915c5133c0f3229a28 » possiblement en lien avec une campagne d'espionnage industriel et de sabotage ciblant la France depuis plusieurs semaines.

[28/02/2020 14:02] Suite à ce signalement, une recherche globale préventive de ces deux indicateurs est lancée sur l'intégralité du parc informatique local.

Schéma infrastructure :

Objectifs :

Par groupe de 3 à 5, vous constituez une équipe de réponse à incident de la société « Alpa37 » mandaté par la société « 42-industrial SA ».

A partir des éléments présentés dans le cours, proposez une démarche que vous appliquerez lors de votre venue sur site afin de répondre au plus vite à cet incident et proposer dans une deuxième partie des recommandations et axes d'améliorations.

Liste Questions/Réponses :

Ci-dessous vous trouverez les échanges que nous avons eu en préparation de notre intervention.

Questions génériques

Organisation

- Connaissez-vous les bonnes pratiques à adopter en cas de suspicion d'attaque informatique ? NON
- Antivirus : date, version, mises à jour. Est-il déployé de partout ? Compatible avec SCADA & systèmes d'exploitation ? Kaspersky pour les Workstation, Symantec pour les serveurs
- Possédez-vous PRA et PCA ? Pas de PRA, ni de PCA
- Etes-vous en conformité avec RGPD ? Qu'avez-vous déjà entrepris ? NON
    - Avez-vous déclaré des traitements de données personnelles auprès de la CNIL ? NON [Déterminer si une déclaration d'incident doit être effectuée auprès de la CNIL]
- Des prestataires sont-ils intervenus ces dernières semaines sur votre infrastructure ? OUI. MAJ tous les 6 mois / Infogérance [Identifier la source de l'infection]

Infrastructures

Pas de supervision spécifique => juste un Zabbix

- Utilisez-vous un outil de gestion de flot, exemple : SCCM ? NON
- Disposez-vous d'un diagramme des flux ? NON
- Avez-vous une cartographie à jour ? NON
- Quelles sont les échanges possibles entre votre réseau de production (Automates, robots ?) et votre réseau bureautique ? Tout est interconnecté, aucune garantie sur les VLAN
- Comment votre réseau local communique avec les serveurs hébergés ? MPLS
    - Quel type de VPN utilisez-vous entre votre entreprise et vos serveurs hébergés ? Aucun
- Avez-vous des sondes sur les firewalls ? OUI : IDS sur Fortinet par défaut
- Pourriez-vous nous fournir un détail des systèmes d'exploitation qui compose vos réseaux ?
  Postes utilisateurs : Windows 10,
  Serveurs : Windows server 2008,
  Production : XP & 2000.
- Pourriez-vous nous fournir un détail des règles de filtrage mis en place pour contrôler vos réseaux ? Aucune idée.
- Avez-vous effectué des tests de backup et de restauration ? De temps en temps par les admins.
- Avez-vous une centralisation des logs ? (Actifs réseau, serveurs) NON
    - Utilisez-vous une méthode pour le traitement des logs ? NON par journalisation par défaut.

Business

- Quelles sont vos contraintes en termes d'interruption de services ? [Déterminer le temps d'interruption acceptable, au cas où] : 1H d'interruption = 100k € de perte.
- Avez-vous la possibilité de déporter une partie de la production vers un autre site ? NON [Déterminer si un plan de secours est possible]

- Quelle est la nature de votre production ? [Déterminer s'il s'agit de matériel critique, dangereux, liée à des activités d'état etc. cf. : la campagne en cours] : Pièce mécanique pour le marché de la robotique

Incident

- Quelles actions ont été entreprises sur le réseau indiquant un potentielle dysfonctionnement : Rien

La personne qui a déclaré le ralentissement :

  - Dans quel bâtiment/site se trouvait-il ? Site principal, sur la machine « historian », puis sur le site A ralentissement d'une machine noté par une responsable production
  - Sur quelle machine travaillait-il ? « historian »
  - Sur quel réseau le ralentissement a-t-il était constaté ? (Production, entreprise ?) Production puis réseau industriel.
  - La machine a-t-elle subit des modifications depuis l'annonce de ce ralentissement ? NON
  - Quelles actions ont été réalisées sur la machine ? Rien, on attendait le conf call
  - Quel système a été impacté par les ralentissements ? Historian
  - Quel type de ralentissement a-t-il constaté ? Fonctionnement plus lent que la normal, diminution de la vitesse de production
  - Après la visite de quel site internet a-t-il détecté des ralentissements ? RDP lent, latence, application métier longue à ouvrir.
  - Après l'installation de quel soft a-t-il détecté des ralentissements ? Aucun
  - A-t-il remarqué une notice d'information (pop-up) de l'antivirus ? Non
  - La machine a-t-elle accès à internet ? [*Identifier la potentiel source d'infection*] On-premise, on ne sait pas si c'est connecté sur internet
  - La machine utilise elle des partages réseaux ? Si oui vers quelles ressources de votre infra ? [*Identifier la propagation*] Oui, business
  - Quelles actions ont été menée depuis la découverte de l'incident [*Déterminer l'origine des modifications/actions/ depuis l'incident*] Rien

Questions phase préparation

- Toutes les collaboratrices et tous les collaborateurs sont-ils conscients des politiques de sécurité de l'Organisation ? Pas de PSSI
- Les collaborateurs savent-ils qui contacter en cas de doute/d'incident informatique ? Oui, les administrateurs
- Pouvons-nous communiquer à l'ensemble des collaborateurs ou responsable… sur l'incident en cours, et sur les éléments concernant la réponse à l'incident ? Uniquement via notre correspondant Yoan ISSARTEL
- Pouvons-nous utiliser/installer nos outils de réponse aux incidents afin de réaliser les différentes phases prévues ? Oui, tout ce que vous voulez.
- Avez-vous une base de connaissance sur des incidents déjà produits ? Sur des réponses à ces incidents ? Non

La démarche

Notre démarche de réponse à incident s'effectuera en 6 étapes :

- 1.Préparation
- 2.Analyse et identification
- 3.Mise sous contrôle ou endiguement
- 4.Eradication
- 5.Remise en état
- 6.Boucle d'amélioration

Dans chaque étape, nous allons vous décrire :

- Les actions en détail
- La ou les raisons des actions
- Les différents scénarios/options suites aux investigations
- L'impact des actions pour votre business, vos productions et vos collaborateurs.

Étape 1 : la préparation

À la suite d'une suspicion d'incident, votre entreprise « *42-industrial SA* », a fait appel à notre entreprise Alpa37. Une équipe de 5 personnes interviendra sur votre site et sera chargé d'y répondre.

Nous devons confirmer le contexte et également recueillir des informations complémentaires.

En prévision de notre intervention, nous vous proposons un meeting (Web/téléphonique) avec une série de questions/réponses. Cet échange permettra d'orienter notre investigation et d'intervenir rapidement, en obtenant des informations plus précises sur cet incident et les impacts potentiels sur votre entreprise.

À la suite de l'échange eu avec le responsable informatique, un second ralentissement a été sur le site A. Afin de s'assurer que cette anomalie ne se soit pas propagée sur le reste de votre entreprise, notre équipe va donc contrôler l'intégralité de votre système d'information. Pour cela, notre équipe va se disperser sur chaque site.

A l'issu de ces étapes, nous déterminerons ainsi l'avancement de l'incident et la démarche à suivre.

Dès la contractualisation de notre intervention, nous avons commencé un travail de recherche sur les indicateurs de compromission que vous nous avez communiqué :

- Exécutable : dem352.exe
- Condensat SHA-1 : f161ebd29699d93411cec0915c5133c0f3229a28

Le NIST a identifié l'exécutable « dem352.exe » comme menace critique.

Dans le cas de la détection d'une compromission dans laquelle une fuite de données à caractère personnelles est identifiée, nous vous fournirons les éléments nécessaires pour engager les démarches auprès de la CNIL.

Pour rappel, toute suspicion ou fuite de données avérées à caractère personnelles doit faire l'objet d'une déclaration auprès de la CNIL dans les 72h.

Étape 2 : Analyse et identification

Il est important que nous puissions :

- Identifier la personne qui a relevé cette anomalie, quel service ? Quel site ?
- Horodater l'heure et la date du constat de l'incident

L'expérience montre que le facteur humain est un élément clef dans ce processus d'alerte : il est essentiel que les employés sachent reconnaître des situations anormales et qu'elles puissent remonter ces informations de façon rapide.

Notre équipe devra rapidement analyser la situation de façon à confirmer la réalité de l'incident, sa nature et son étendue

Dès notre arrivé, nous allons réaliser une recherche préventive sur l'intégralité du parc informatique à l'aide des indicateurs déjà connu :

- Exécutable : dem352.exe
- Condensat SHA-1 : f161ebd29699d93411cec0915c5133c0f3229a28

Pour cela, nous devrons déployer une application (Mozilla investigator) packagée selon les différents OS sur chacun des actifs du système d'information. Ce déploiement pourra se faire soit via GPO, soit par SSH, soit manuellement (clé USB). Une fois cet agent déployé, nous pourrons lancer des recherches en parallèle sur l'intégralité du parc.

En faisant une corrélation des retours de cette recherche, cela permettra de répondre aux questions suivantes :

- Est-ce un incident ? Si oui est-il globalisé ?
- Quelles sont les machines qui sont infectées ? A quels services appartiennent-ils ?

Suivant le nombre de machines infectées, il faudra catégoriser et déclencher un incident de lutte informatique défensive au niveau de l'entreprise. Il faudra aussi réaliser une communication auprès des utilisateurs.

Après en avoir informé la personne référence sur site, le plan de réponse devra être validé. Il s'en suivra une phase de mise sous contrôle.

Étape 3 : la mise sous contrôle ou endiguement

La phase de mise sous contrôle ou d'endiguement vise à stabiliser l'environnement de sorte que le problème ne s'aggrave pas. En fonction de la nature de l'incident, un système compromis peut être isolé du réseau ou des flux coupés au niveau d'un firewall.

Un élément important de cette phase est de conserver une liste la plus complète possible de tous les changements effectués sur l'environnement concerné, afin d'être en mesure de remettre à leur état initial les systèmes et de déterminer de façon fiable les changements effectués par l'attaquant.

Lors de cette étape, nous allons approfondir nos connaissances sur l'incident, la menace et son impact. Ces informations seront précieuses lors de la phase suivante qui vise à éradiquer la menace de l'environnement ciblé.

Identification de la menace :

Comme expliqué ci-dessus, nous réaliserons une analyse complète de la menace. Le but sera pour nous de :

- Dresser un profil de cet exécutable (emplacement, mode d'exécution, ses actions, fréquence d'exécution, mode de communication, etc.)

Pour dresser ce profil, nous allons d'abord isoler la ou les machine(s) infectée(s) afin de réduire sa propagation au sein de votre infrastructure (communément appelé analyse de la menace).

Une fois que nous aurons une idée plus précise de cet exécutable, nous analyserons les machines infectées.

Un travail d'investigation numérique sera nécessaire sur cet exécutable pour répondre à ces questions:

  - Que fait l'exécutable ?
  - Quels sont les impacts sur votre système d'information ? (Récupération de données confidentielles ? Backdoor pour une attaque future ?)

Une fois fait, nous analyserons la mémoire de la machine afin de voir si des liens sont présents entre l'exécutable et des services, des processus, des programmes, des bibliothèques, clefs de registre…

- Déterminer l'impact sur votre système d'information (réseau, bande passante, etc.).

Nous pourrons ainsi qualifier l'impact de la menace sur votre SI, déterminer sa criticité et la nécessité ou non d'interrompre la production.

Il s'en suivra d'une phase de confinement, qui s'effectuera en deux temps :

- Phase de confinement à court terme
- Phase de confirment à long terme

Confinement à court terme

Afin de confiner l'exécutable, une étape de confinement à court terme doit avoir lieu, d'autant plus que vous avez constaté un second ralentissement sur un site différent.

Il est donc important d'endiguer la propagation dans le cas éventuel d'une infection.

Pour cela, selon les éléments recueillis dans la phase d'étude sur le comportement de l'exécutable, nous devrons isoler le poste contaminé du reste du système d'information.

Deux options sont possibles :

Option 1 :

Le poste peut être isolé sans impacter la production. Cette solution permettrait d'intervenir rapidement et de sécuriser votre SI.

Option 2 :

Le poste est primordial à la production et ne peut être interrompu. Il sera donc nécessaire de travailler avec les propriétaires du système ou le(s) gestionnaire(s) pour déterminer des mesures supplémentaires nécessaires pour contenir le problème.

Dans ce cas, il sera donc essentiel qu'une solution alternative soit trouvée pour contenir cette menace, sans arrêt de production.

Remarque : tous les postes présentant des signes d'infections doivent être isolés pour être dans l'incapacité de propager la menace.

Confinement à long terme

Option 1 :

- Si le système peut être mis hors ligne, on passe à la phase d'éradication.

Option 2 :

- Si le système doit rester en production, on procède à un confinement à long terme en supprimant tous les logiciels malveillants et autres artefacts des systèmes affectés, et durcir les systèmes touchés d'autres attaques jusqu'à ce qu'une circonstance idéale permette de réimagé les systèmes touchés.

Étape 4 : l'éradication

Pour l'éradication de la menace, nous vous proposons 2 options possibles, l'une radicale que nous conseillons et garantissons, l'autre qui sera un nettoyage de la machine.

Option 1 :
Nous réaliserons à vos côtés un formatage de la machine infectée, puis nous passerons à l'étape 5 qui concerne le retour à la normale.

Option 2 :
Plusieurs contrôles seront réalisés lors du nettoyage pour s'assurer que la menace est bien supprimée.

En effet, il est important de s'assurer que tout sera fait pour éviter que le même problème ne revienne après. Si une vulnérabilité connue a été utilisée pour pénétrer le système, il faudra installer les correctifs et les outils nécessaire à la détection de cet incident.

Avoir un incident de sécurité est une chose, que celui-ci se reproduise est encore plus dérangeant.

Etape 5 : la remise en état

Une fois que la cause de l'incident a été identifiée et les causes corrigées, il s'agit de remettre le système en état de bon fonctionnement afin de permettre le retour à la normale et que vous puissiez reprendre vos activités.

Option 1 :

Une fois la machine formatée, nous réaliserons à vos côtés et selon votre mode de déploiement une installation complète de la machine. Nous confirmerons la « bonne santé » de cette machine dorénavant « saine » afin de remettre en production la machine.

Option 2 :

Il conviendra d'être particulièrement vigilant et de surveiller toute nouvelle tentative d'intrusion ou d'infection. En effet, il est tout à fait possible que les travaux de nettoyage prennent un certain temps (déploiement de correctifs sur un grand nombre de systèmes), ce qui pourrait être une opportunité pour un attaquant de revenir ou une infection de resurgir de façon soudaine.

- Retour à la normale

Une fois le retour à la normale de la production, nous mettrons en place avec votre accord, différentes solutions au sein de votre système d'information pour vérifier que l'incident ne se reproduise pas.

Nous vous aiderons à configurer votre solution de supervision (Zabbix) pour que celle-ci vérifie la non-présence des différents éléments concernant cet incident.

Une tâche planifiée pourra aussi être créée afin de vérifier sur la machine anciennement infectée que la menace est réellement supprimée, et ce, sur un temps donné (3 semaines de préférences).

Étape 6 : la boucle d'amélioration

Cette dernière phase vise à effectuer un retour d'expérience afin d'analyser de façon objective et honnête comment l'incident a été géré. Il s'agit d'identifier :

- Ce qui a bien fonctionné,
- Ce qui pourrait être amélioré,
- Ce qui n'a pas du tout fonctionné.

La fin de l'intervention conduira à la remise d'un rapport, lors d'une réunion, dans lequel sera détaillé les différentes actions menées. Cette documentation sera à conserver dans une base de connaissance qui permettra une réactivité plus rapide sur ce type d'incident.

Ce retour d'expérience nous permettra :

- D'avoir votre ressenti sur notre intervention
- D'améliorer nos modes d'intervention.
- De vous présenter nos propositions et axes d'améliorations

Propositions et recommandations

Durant notre analyse, nous avons pu relever certains points qui pourront être améliorés. Ces points couvrent les infrastructures en place et vos processus en cas d'incidents.

Parmi les points abordés par notre audit, nous vous proposons plusieurs axes d'améliorations :

Organisationnel

Pour vos futurs projets et dans un souci d'amélioration continu, nous vous recommandons de mettre en place une démarche ITIL. Cette démarche a pour but, la mise en place un processus de gestion des incidents. Ainsi, votre DSI sera en mesure de les gérer plus efficacement.

Une fois cette étape réalisée, nous vous accompagnerons pour la mise en place d'autres processus tel que la gestion des évènements, qui sera basée sur votre outil de supervision : Zabbix.

Lors de nos échanges, vous nous avez confié que vous réalisez de simple « ping » vers les équipements pour contrôler leurs états. Nous vous recommandons d'affiner et d'améliorer vos contrôles.

ZABBIX est un logiciel libre permettant de surveiller sous forme d'alertes l'état de divers services réseau, serveurs et autres matériels réseau et produisant des graphiques dynamiques de consommation des ressources. Il peut par exemple effectuer les contrôles suivants :

- Systèmes (CPU, processus, température, mémoire, trafic…)
- Serveurs web (Apache, Lighttpd…)
- Serveurs de base de données (MySQL, PostgreSQL, Oracle…)
- Serveurs de messagerie (Postfix, Amavis…)
- Application Java (Tomcat, JBoss, Hibernate…)
- Autres éléments réseaux : Imprimantes, Onduleurs, Switch, Routeurs, IPBX…
- Création de plugins personnalisés afin de monitorer vos services spécifiques

Depuis le 25 mai 2018, la nouvelle réglementation européenne de la sécurité des données à caractère personnel est entrée en vigueur. Nous vous recommandons d'entamer des démarches de mise en conformité vis-à-vis de cette réglementation. Toute entreprise n'étant pas en conformité avec celle-ci, risque alors une amende à hauteur de 2 à 4 % de son chiffre d'affaire ou 10 à 20 millions d'euros. Le montant le plus haut sera retenu.

Il est fortement recommandé de rédiger une PSSI. Elle vous permettra de formaliser la stratégie de l'entreprise par rapport à la sécurité du SI.

Nous vous recommandons de réaliser au moins un audit de sécurité un fois tous les six mois. Il est préférable qu'il soit réalisé par une entreprise externe.

Il est important d'effectuer une campagne de sensibilisation auprès de vos collaborateurs. Cette étape est nécessaire pour les responsabiliser sur les risques et menaces informatiques. Ainsi, ils sauront réagir à ces menaces.

Infrastructures

Lors de notre échange, vous nous avez relaté que des interventions, datant de 6 mois, de prestataires externes ont eu lieu sur votre système, sans connaitre les actions effectuées. Afin de garantir une qualité de suivi, nous vous recommandons l'intégration de fiches d'interventions, afin d'engager la responsabilité de vos prestataires sur vos actifs (actifs réseaux, serveurs, postes des utilisateurs, automates…).

Nous vous recommandons, la mise en place d'un SIEM qui aura pour but de corréler, de centraliser et d'analyser l'intégralité des logs avec la mise en place d'alertes, pour détecter des « comportements anormaux », sur ces actifs.

De plus, pour réaliser une gestion efficace de votre parc, le déploiement d'un outil de gestion de système tel que SCCM (logiciel de Microsoft) est primordiale. Cet outil vous permettra de gérer efficacement l'intégralité de vos postes Windows. Il s'agit par exemple de contrôler les mises à jour Windows, les logiciels installés ou tester la conformité de vos postes serveurs et clients.

Concernant la gestion des antivirus qui a retenu notre attention, nous vous préconisons d'en installer qu'un seul sur l'ensemble de votre parc. Cela vous apportera une meilleure visibilité, une gestion et un contrôle simplifiés et une plus grande protection de votre système informatique, au travers d'une seule console de management.

Vous étiez également dans l'incapacité de nous fournir une liste détaillée des règles de filtrage implémentées sur vos équipements et vos réseaux. Nous vous proposons de vous accompagner dans la création d'un diagramme des flux et contrôler avec vous, le paramétrage de vos équipements filtrants. Par la suite, vous serez en mesure d'entreprendre la cartographie complète de votre SI.

Enfin, nous vous recommandons de planifier en début de mois, des tests de restaurations. Vous aurez ainsi la certitude que vos sauvegardes sont fiables et fonctionnelles.

Business

Actuellement, vous ne disposez pas de plan de continuité informatique (PCI) et plan de reprise informatique (PRI). Or, lors de notre dernier échange, vous avez soulevé le fait qu'une heure d'interruption de service représentait pour votre entreprise une perte financière de 100.000 euros par heure.

Dans le but de garantir une continuité de service, nous vous recommandons fortement la mise en place d'une solution pour réduire les risques entrainant cette perte financière. Nous vous proposons un accompagnement pour déployer ce PRI/PCI.

Outils utilisés

Voici la liste des outils que nous serons amenés à utiliser lors de notre intervention :

Acquisition

- Récupération des données originales (copie "physique" - Tout le disque, copie "logique" - Une partition d'un disque)

Logiciels : AccessData FTK / EnCase / Wireshark
Matériels : Logicube Talon / VOOM HardCopy3 / ImageMASSter Solo III Forensic
Il faut tout de même un logiciel pour analyser les données

Validation et "discrimination" (tri + recherche)

- Vérification de l'intégrité des données copiées
    - "Hashing", filtrer, analyse des en-têtes,
    - Tri+ recherche dans les données récupérées pour l'investigation
- Suppression des données "saines", recherche des données "corrompues"/suspectes

Extraction

- Récupération des données utiles
- Analyse des données
- Recherche de "mots clés", de type de fichiers particuliers
- Déchiffrement

Logiciels : ProDiscover / X-WAYS Forensics / FTK / EnCase / Volatility / Wireshark

Reconstruction

- Création d'un élément suspect en fonction des analyses faites pour "voir ce qu'il se passe" lors d'un incident
- Duplication de l'élément pour des investigations ultérieures
    - Copie disque > disque
    - Copie image > disque
    - Copie partition > partition

Matériels : Logicube Talon / Logicube Forensic MD5 / ImageMASSter Solo III Forensics

Logiciels : EnCase / FTK Imager / ProDiscover / SnapBack

Reporting

- Extraire les "preuves", les logs de l'incident manuellement (Rapport des logs) / copier les données suspectes dans un autre programme pour créer un rapport (PDF, Word, HTML...)