Présentation de la solution ESG

Architecture de sécurité adaptative Cisco

Date : février 2015Auteur : Jon Oltsik, analyste principal sénior

Résumé : *Les entreprises sont aujourd'hui confrontées à un paysage de menaces sans précédent, qui sont à l'origine de la récente vague de violations de données comme chez Target, Home Depot et JPMorgan Chase. Face à cette situation, les directeurs de la sécurité des systèmes d'information ne doivent plus considérer les contrôles de sécurité uniquement à des fins de prévention. Les entreprises doivent en outre traquer de manière proactive toute activité malveillante par la collecte et l'analyse des données de sécurité à la fois internes et externes. Pour cela, les directeurs de la sécurité des systèmes d'information doivent mettre en place une architecture de sécurité active et adaptative prenant en charge l'ensemble des terminaux, des réseaux, des analyses de sécurité, des technologies avancées de prévention et de détection des programmes malveillants et des informations externes sur les menaces. Pour répondre à ce nouveau besoin des entreprises, Cisco a développé sa propre architecture, qui regroupe les meilleurs produits, services et partenariats.*

Présentation

D'après le rapport que Verizon a publié en 2014 sur les incidents liés à la sécurité des données (Data Breach Investigation Report), 75 % de toutes les violations de données ne sont découvertes que dans un délai de plusieurs semaines, voire de plusieurs mois. Le temps actuellement nécessaire entre une attaque malveillante initiale et sa détection effective est le principal facteur aggravant de la vague de violations de données, à la fois visibles et onéreuses, qu'ont subie l'année dernière des entreprises comme Target, Home Depot, JPMorgan Chase, Sony Pictures et Staples.

Cette situation pose une question essentielle : alors que les entreprises dépensent chaque année des millions de dollars pour assurer la sécurité des informations, pourquoi le temps nécessaire à la détection des violations de données est-il si long? D'abord, de nombreuses entreprises éprouvent encore des difficultés à réunir les compétences, les procédures et les technologies nécessaires de détection des incidents et de remédiation.

Les recherches d'ESG permettent d'illustrer ce phénomène. Dans le cadre d'une étude d'ESG, il a été demandé aux professionnels de la sécurité de préciser leurs points faibles en matière de détection et de gestion des incidents. Selon les données recueillies (voir la figure 1) :

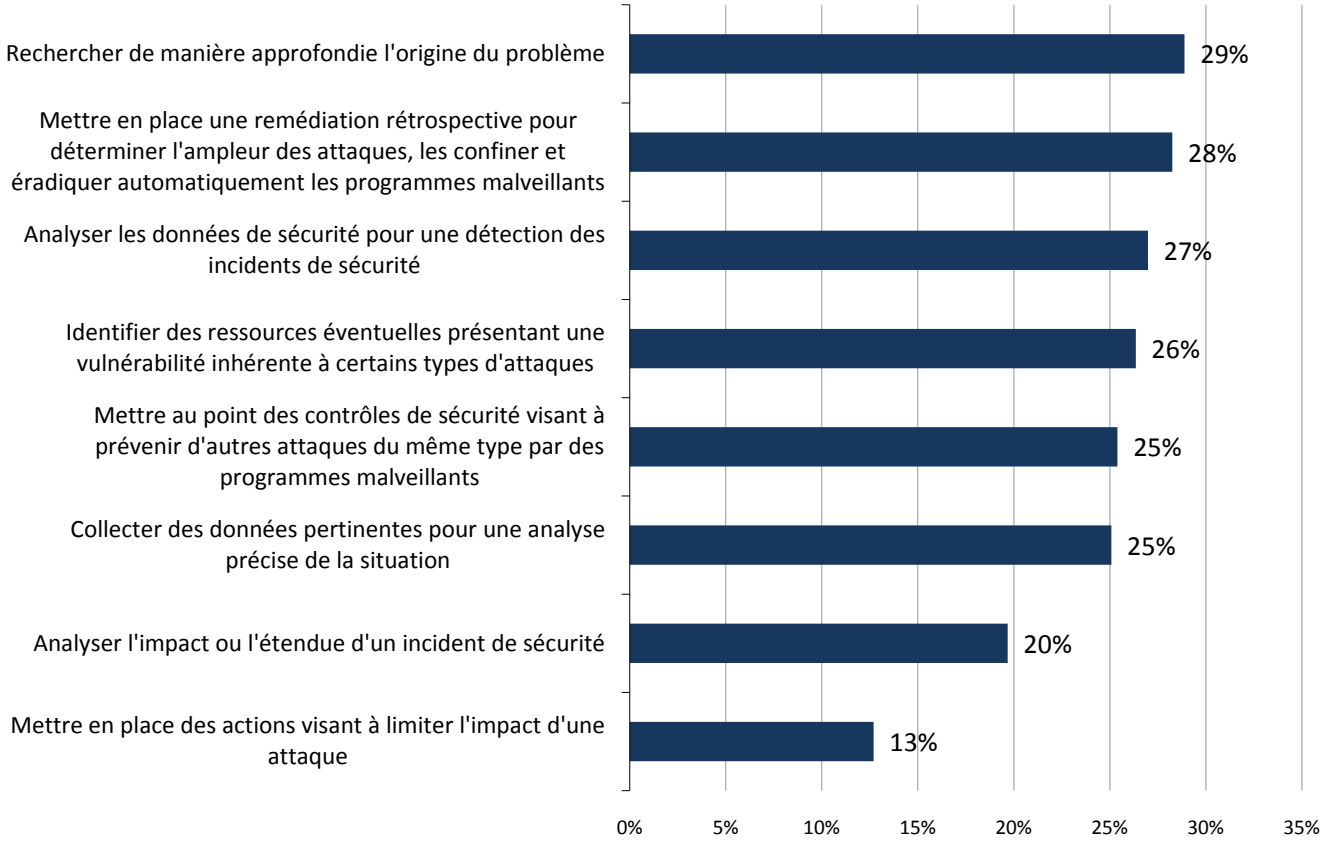
- 27 % des entreprises estiment éprouver des difficultés en termes d'analyse des données de sécurité à des fins de détection des incidents. Cela s'explique principalement par un manque de compétences solides dans l'analyse de la sécurité;
- 29 % des entreprises considèrent ne pas être suffisamment efficaces dans la recherche de l'origine des problèmes. Cela peut également être dû à des problèmes liés aux compétences, mais aussi à une trop grande confiance dans d'anciens outils d'analyse de sécurité ou à des problèmes de pertinence dans la collecte et l'analyse des données ;
- 28 % des entreprises indiquent ne pas savoir tirer pleinement parti de la remédiation rétrospective pour déterminer l'ampleur des attaques, confiner les menaces et éradiquer les programmes malveillants. Autrement dit, elles ne sont pas en mesure d'exploiter efficacement les analyses historiques ou de mettre en corrélation les activités des terminaux, le trafic réseau et les informations sur les menaces.[1]

Les professionnels de la sécurité ont par ailleurs signalé un nombre important d'autres points faibles liés à la détermination des ressources vulnérables, à la mise au point des contrôles de sécurité et à la collecte de données exploitables.

[1] Source : ESG Research Report, *Advanced Malware Detection and Protection Trends*, septembre 2013.

Figure 1. Points faibles en matière de détection et de gestion des incidents

Sur la base de cette liste de tâches de détection et de gestion des incidents, choisissez les trois tâches que vous considérez comme les points faibles de votre entreprise (c.-à-d. celles dans lesquelles vous n'êtes pas suffisamment efficaces)? (Pourcentage de personnes interrogées, N=315, trois réponses acceptées)



Source : Enterprise Strategy Group, 2015.

Les données d'ESG mettent en avant différents problèmes communs de détection et de gestion des incidents qui touchent à la fois les personnes, les processus et les technologies. Cela n'est toutefois pas étonnant dans la mesure où :

- **Les professionnels compétents en matière de cybersécurité sont peu nombreux.** Une autre étude d'ESG révèle que 28 % des entreprises souffrent d'une pénurie problématique de personnel compétent en sécurité informatique.[2] Ces compétences en sécurité informatique sont en fait citées comme les compétences dont la pénurie est la plus problématique par les personnes interrogées dans l'étude annuelle d'ESG sur les dépenses informatiques prévues, et ce pour la quatrième année d'affilée. Pour résumer, quelle que soit leur taille, les entreprises ne parviennent pas à trouver ou à recruter des professionnels de la sécurité disposant des compétences appropriées d'analyse de la sécurité, ce qui les rend d'autant plus vulnérables aux cyberattaques.
- **Les procédures restent manuelles et réactives.** Plutôt que de traquer les activités anormales ou suspectes, de nombreuses entreprises ne mettent en place des mesures de recherche ou de remédiation qu'après une violation de données avérée. Une fois les premières mesures engagées, les analystes sont souvent contraints par des outils de sécurité limités dans le temps et des procédures manuelles fastidieuses. Cela ne fait qu'augmenter la durée des recherches et des efforts de remédiation, comme le décrit le rapport Data Breach Investigations Report de Verizon.

[2] Source : ESG Research Report, *2015 IT Spending Intentions Survey*, février 2015.

- **Les technologies de sécurité restent axées sur la prévention.** Les technologies de prévention comme les pare-feu, les systèmes IDS/IPS et les antivirus jouent en effet un rôle important, mais un trop grand nombre d'entreprises concentrent trop leur temps et leur argent dans ce type de solutions. Dans l'état actuel du paysage des menaces, les directeurs de la sécurité des systèmes d'information doivent accepter que leurs réseaux seront un jour compromis et consacrer les ressources nécessaires dans des systèmes de détection et de résolution des incidents.

Sécurité active et adaptative

Il va de soi que les professionnels de la sécurité doivent appliquer des contrôles de sécurité adaptés pour bloquer les programmes malveillants classiques et les types de cyberattaques les plus courants dans leur secteur d'activité. Les entreprises du secteur du commerce auraient ainsi tout intérêt à exécuter des contrôles d'applications sur les systèmes de point de vente et à mettre en place des règles pour leur pare-feu réseau garantissant que seuls les terminaux point de vente pourront s'y connecter à partir d'adresses IP de confiance. Au-delà de la simple prévention, les directeurs de la sécurité des systèmes d'information doivent adopter une approche plus proactive en supposant que leurs entreprises constituent des cibles de choix qui peuvent être victimes d'attaques à n'importe quel moment. Cela sous-entend une recherche proactive et continue de tout comportement anormal et une capacité à procéder rapidement à une validation et à un examen complet de la situation lorsque cela est nécessaire.

Pour atteindre ces objectifs, les directeurs de la sécurité des systèmes d'information doivent s'engager à améliorer la collecte et l'analyse des données de sécurité venant de sources internes comme externes. Les équipes de sécurité doivent en outre mettre en place un flux de travaux intégré pour la détection et la gestion des incidents. Ces efforts nécessiteront une architecture de sécurité réunissant les avantages suivants :

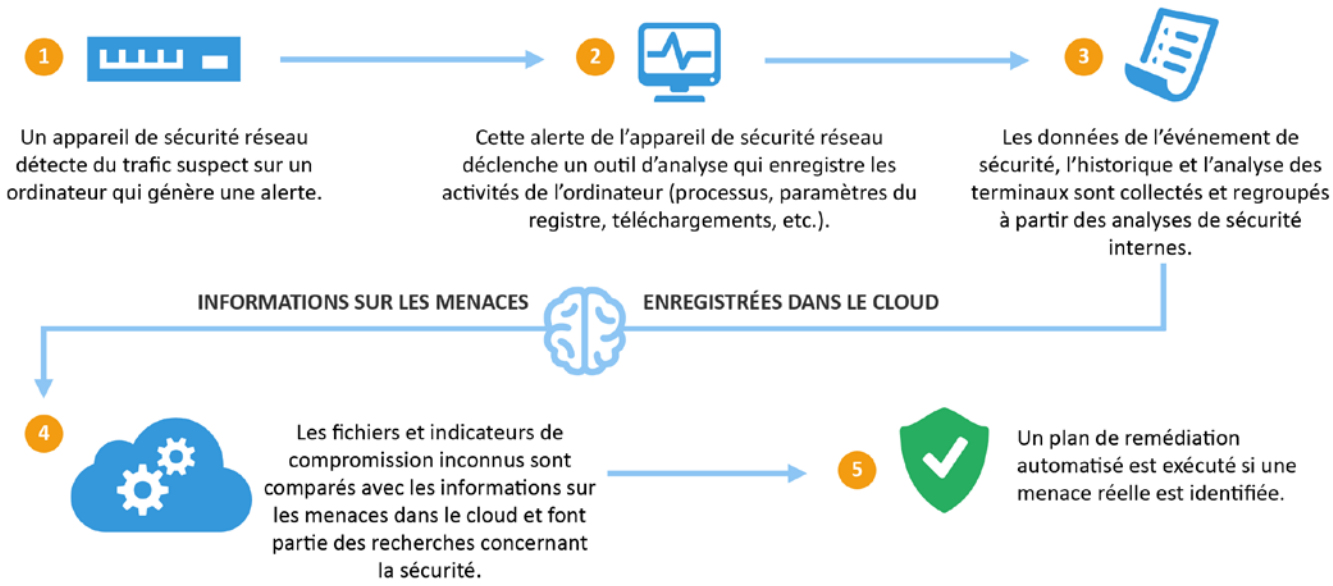
- **Une surveillance continue.** Les outils de traque peuvent mettre en évidence de nombreux indices essentiels en examinant les activités de l'ensemble des terminaux et des réseaux. Les outils de capture analytique peuvent par exemple consigner des événements aussi variés que les téléchargements, les modifications du registre, les processus de mise en mémoire ou les connexions réseau. De la même manière, les outils d'analyse du réseau permettent de surveiller les données NetFlow ou de contrôler les paquets IP afin de préciser les informations relatives aux connexions, aux sessions, aux ports et aux protocoles des couches ISO 2 à 7. Forts de ces données, les analystes de la sécurité peuvent enrichir les alarmes et les données des événements de sécurité de base par le biais d'enregistrements historiques complets sur les circonstances d'un incident.
- **Une analyse statique et dynamique des fichiers.** Les entreprises doivent être en mesure de déterminer si des fichiers sont inoffensifs ou dangereux, qu'ils soient transférés par courriel, via des liens hypertextes, etc., et ce quel que soit leur format. Ce processus doit également inclure une analyse statique et dynamique des fichiers, sur la base de leur réputation, de leur date de compilation, de la recherche textuelle et de l'émulation d'une exécution dans un environnement virtuel.
- **Un partage des informations sur les menaces.** Bien que l'analyse des données internes soit essentielle, de nombreuses entreprises tirent parti d'informations externes sur les menaces pour mettre leurs données au niveau du réseau en adéquation avec les activités extérieures à leur périmètre. Des connexions réseau suspectes peuvent par exemple être mises en corrélation avec des informations sur les menaces afin de déterminer si une adresse IP cible renvoie vers un site web douteux ou vers un serveur de commandement et de contrôle (C2). Les analystes de la sécurité doivent être en mesure de consulter des informations externes sur les menaces dans le cadre de leurs recherches, mais aussi de partager leurs données internes avec des fournisseurs de services de sécurité tiers ou des centres d'analyse et de partage d'informations sectorielles (Industry Information Sharing and Analysis Centers, ou ISAC).
- **Des règles de déclenchement pour la capture et l'analyse de données.** Toute alerte signalant un événement de sécurité potentiel doit immédiatement déclencher des actions de capture et d'analyse des données. Par exemple, lorsqu'un système IPS génère une alerte à la suite de la détection de trafic réseau suspect, des outils d'analyse des terminaux peuvent être exécutés pour récupérer des données sur les ports ouverts, les processus en cours, les DLL utilisées et les connexions réseau. Cette série d'actions peut

permettre aux entreprises d'automatiser les recherches de sécurité et d'améliorer ainsi l'efficacité de la détection et de la gestion des incidents.

- **Une remédiation automatisée.** Dans la mesure où les entreprises collectent et analysent de plus en plus de données internes et externes, elles ont la possibilité d'automatiser certains processus et d'accélérer les opérations de remédiation. Lorsque du trafic suspect est repéré, des échantillons sont envoyés pour analyse. L'équipe responsable de la sécurité peut importer les résultats d'analyse dans l'infrastructure IT afin d'interrompre les connexions, de générer une nouvelle signature IDS et d'ajouter de nouvelles règles au pare-feu.
- **Des indicateurs de compromission.** Les technologies en place devraient être capables de rechercher en permanence d'éventuels indicateurs de compromission (Indicators of Compromise, ou IoC), qu'ils soient statiques ou comportementaux. Ces indicateurs servent souvent d'indices aux équipes de sécurité pour préciser les systèmes compromis. Leur objectif n'est pas de fournir une liste supplémentaire d'alertes à analyser, mais plutôt de présenter une vue corrélée et hiérarchisée des activités liées aux attaques et aux compromissions.

Pour être réellement efficaces, tous les dispositifs technologiques décrits ci-dessus doivent fonctionner en étroite collaboration sous la forme d'une architecture intégrée d'analyse de sécurité (voir la figure 2). De cette manière, les terminaux, les contrôles de sécurité réseau, les systèmes de protection contre les programmes malveillants, les informations sur les menaces et les analyses de sécurité participeront tous à l'amélioration de l'efficacité, à la pertinence et à la rapidité des processus de détection et de gestion des incidents.

Figure 2. Flux de travaux de sécurité active et adaptative pour la détection et la gestion des incidents



Source : Enterprise Strategy Group, 2015.

La solution Cisco

Les professionnels de la sécurité prennent conscience qu'ils ont besoin d'une sécurité active et adaptative, mais ne savent souvent pas par où commencer ni comment l'incorporer à leur infrastructure tout en garantissant son intégrité et sa cohérence. Cisco a pour mission d'aider les directeurs de la sécurité des systèmes d'information à relever ce défi pour leur assurer une détection et une gestion efficaces des incidents. Au cours des dernières années, Cisco a acquis différents fournisseurs de solutions technologiques de sécurité de pointe et a établi des partenariats avec d'autres afin de rassembler de nombreuses pièces disparates en une architecture de sécurité unifiée et adaptative intégrant les fonctionnalités suivantes :

- **Contrôles de sécurité de réseau.** Fruit de l'acquisition de Sourcefire en 2012, le système IPS de nouvelle génération de Cisco (FirePOWER) est basé sur un ensemble de règles d'informatique de source libre et a été conçu pour une protection contre les menaces sur plusieurs niveaux. S'alignant sur le flux de travaux décrit précédemment, FirePOWER détecte le trafic suspect et génère des alertes.
- **EnCase Cybersecurity de Guidance Software.** Cisco a récemment annoncé qu'il avait établi un partenariat avec Guidance Software en vue d'intégrer son système d'analyse des terminaux (EnCase Cybersecurity) à son architecture de sécurité active et adaptative. Une fois qu'une alerte a été générée par FirePOWER, EnCase Cybersecurity entre en action, enregistre une image instantanée du terminal suspect et rassemble les données pour analyse.
- **AMP Threat Grid.** Tirant parti de données détaillées d'analyse, les analystes de la sécurité examinent les indicateurs de compromissions (fichiers de hachage, DLL ou processus suspects, ou connexions réseau à des adresses IP inconnues) et les comparent aux sources d'information externes sur les menaces afin de repérer d'éventuels comportements malveillants. L'architecture Cisco intègre la solution AMP Threat Grid à cet effet. Les analystes peuvent accéder à AMP Threat Grid depuis EnCase Cybersecurity à partir d'un simple clic droit dans cette dernière application.
- **AMP for Endpoints.** AMP for Endpoints contrôle en permanence les terminaux, bloque les attaques connues, analyse plus de 400 attributs de fichiers en vue de détecter les programmes malveillants, puis met en évidence tout comportement dangereux afin d'aider les entreprises à améliorer, voire à automatiser, la remédiation. AMP for Endpoints assure également un suivi des activités des terminaux pour une remédiation rétrospective. Lorsque de nouvelles variantes de programmes malveillants sont détectées, AMP consulte sa base de données afin de vérifier si des terminaux ne présentaient pas par le passé des indicateurs de compromission caractéristiques de ces nouveaux programmes malveillants. Le cas échéant, AMP alerte l'équipe de sécurité et les guide tout au long de la procédure de remédiation.

Cisco étend également son architecture active et adaptative à certains partenaires du même écosystème. Cisco travaille ainsi en étroite collaboration avec Lancope et Splunk. Ces deux partenaires ajoutent de la valeur à notre architecture en y ajoutant des fonctions complémentaires d'analyse de sécurité.

Conclusions

La sécurité des entreprises suit depuis des années un cycle pour le moins répétitif. Les équipes de sécurité consacraient la plupart de leur temps et de leurs ressources à mettre au point des contrôles de sécurité pour mieux gérer les risques et prévenir les incidents. Lorsqu'un nouveau type de menace faisait son apparition, elles renforçaient simplement le réseau en installant une passerelle supplémentaire, en créant une nouvelle règle de pare-feu ou en ajoutant un nouveau logiciel sur les terminaux.

Cette stratégie a malheureusement montré ses limites. Les directeurs de la sécurité des systèmes d'information doivent considérer que leurs réseaux seront un jour la cible d'attaques sophistiquées et d'assaillants particulièrement déterminés.

Comme le disait Sun Tzu : « Si vous connaissez vos ennemis et que vous vous connaissez vous-même, mille batailles ne pourront venir à bout de vous ». Appliquée à la cybersécurité, cette maxime signifie que les entreprises doivent comprendre le fonctionnement normal de leur réseau, être capables de détecter rapidement les anomalies, puis effectuer des recherches approfondies afin de préciser des problèmes et d'y remédier. Cela n'est possible que si les analystes de la sécurité sont en mesure de collecter, d'analyser et d'exploiter les données de sécurité de manière prompte et pertinente.

La vision d'ESG en matière de données de sécurité active est conçue pour satisfaire ces besoins en associant les données et les actions sur les réseaux et les terminaux à des informations sur les menaces et sur les analyses de sécurité. Il semble évident que toutes les entreprises auront besoin d'une architecture de bout en bout intégrée capable de rassembler tous ces composants. Cisco a bien conscience de cet enjeu et travaille activement au développement d'une solution architecturale intégrant produits, services et partenariats. Cisco Platform Exchange Grid (pxGrid) est un exemple de cette initiative. Cisco pxGrid offre une plateforme de partage de contexte qui peut être exploitée par des solutions partenaires pour l'échange de données contextuelles collectées à des fins d'amélioration de la sécurité. L'écosystème de partenaires Cisco permet une intégration avec de nombreux types de technologies, comme les plateformes de gestion de la mobilité en entreprise et de gestion des appareils mobiles, la gestion des événements et des informations de sécurité, la gestion des identités et de l'accès, l'évaluation des vulnérabilités, l'analyse de la sécurité et du réseau, ou encore les technologies opérationnelles. Les directeurs de la sécurité des systèmes d'information cherchant à mettre en œuvre une architecture de sécurité active et adaptative trouveront ainsi une solution parfaitement adaptée à leurs besoins parmi les offres Cisco.