ENJOY SAFER TECHNOLOGY™

Communiqué de presse

Septembre 2019

ESET Security Day de Tunis 2019 : une journée pour faire le point sur la cybersécurité

Quelle évolution pour la cybersécurité en 2019 ? Quelles nouvelles attaques ? Comment se protéger ? Un panel d'experts s'est réuni à Tunis à l'occasion du ESET Security Day 2019. Au programme : menaces, solutions et prise de hauteur avec le Dr Patrice Guichard et l'expert en cybersécurité Benoit Grunemwald.

Pour la 3e édition des ESD Tunis, ESET revient au cœur du quotidien des RSSI : concilier d'une part la connaissance des menaces avancées qui défraient la chronique et d'autre part assurer la gestion du parc existant, avec ses exigences plus prosaïques, telles que veiller à limiter l'impact du client antivirus sur les performances de systèmes parfois vieillissants !

Avec 30 ans d'expérience dans la recherche cybersécurité et le développement de solutions de protection des postes de travail, ESET est précisément au cœur de cette double exigence. C'est d'ailleurs pour cela que l'analyste **Gartner** l'a nommé pour la seconde année consécutive « *Challenger* » dans son étude sur les solutions de protection des postes de travail.

Les chercheurs d'ESET assurent une veille permanente sur les nouvelles menaces, traquent les groupes d'attaquants avancés, identifient leurs nouveaux outils, et sont à l'origine de très nombreuses publications exclusives, que l'on retrouve notamment sur le blog WeLiveSecurity.

Toute cette connaissance — et plus encore — est mise à la disposition des entreprises dans l'offre de **Threat Intelligence** d'ESET. Une offre de Big Data sur les toutes dernières menaces, qualifiées, immédiatement exploitables par les RSSI pour évaluer l'exposition au risque de leur organisation ou connaître tous les secrets des attaquants.

Thématique 1 | État des lieux sur les menaces et techniques des cybers criminels, Dr Patrice Guichard
Connaissez-vous les TTPs ? Ce sont les « techniques, tactiques et procédures » des cybercriminels. Autrement dit, le détail des méthodes qu'ils mettent en œuvre pour pénétrer les entreprises. Et lorsque l'on se penche sur le sujet, nous sortons du cadre plutôt commun du fichier malveillant (le virus) détecté par un antivirus traditionnel. Les attaquants vont aujourd'hui beaucoup plus loin, et c'est ce que nous montre le Dr Patrice Guichard à travers des exemples — anonymes bien sûr — rencontrés sur le terrain durant ses investigations numériques. Le tout avec un seul objectif : que les participants puissent répondre à la seule question qui compte : « *quels sont les maillons faibles au sein de mon organisation et comment les transformer en atout* ? ».

Thématique 2 | Ransomware, anticipation et mesures post-attaques
Les ransomwares frappent aveuglément aussi bien les particuliers que les entreprises en détruisant de précieux contenus. Il n'est pas rare qu'une infection par ransomware fragilise une petite entreprise au point de menacer sa survie.
Il est alors indispensable d'apprendre à s'en protéger. Pour cela, une sandbox dans le Cloud peut déjà être fort utile : les ransomwares, mais aussi les autres menaces inconnues de type APT, seront filtrées dans le nuage avant de pouvoir arriver dans la boîte email de l'utilisateur.
Mais tout RSSI sérieux souhaitera bien entendu aller plus loin. Il voudra avoir une visibilité absolue sur tout ce qui se passe sur ses postes de travail, en mode « tour de contrôle » numérique, et disposer de moyens d'action immédiats pour agir le cas échéant. C'est ici le rôle des solutions de détection et de réponse (EDR) ESET, associées à la puissance d'une analyse dans le Cloud, alimentée en temps réel par les détections des centaines de milliers de postes de travail et par les découvertes des chercheurs ESET.
Malgré tout, un poste mal protégé peut toujours être victime d'un ransomware. Dans cette situation, bien qu'il ne soit pas conseillé de payer la rançon, la décision ultime appartient au dirigeant (s'il dispose de bonnes sauvegardes déconnectées et vérifiées, il s'en sortira bien !)
Mais quoi qu'il décide, la remédiation sera chronophage ! Cela s'anticipe donc en préparant un PRA (Plan de Reprise d'Activité), qui aura pour objectif d'assurer la cyber-résilience de l'entreprise en lui permettant de restaurer au plus vite les machines touchées.

Thématique 3 | SOC : Méthodologie pour centraliser et maitriser sa sécurité
Le SOC (Security Operation Center) est une véritable tour de contrôle qui surveille l'ensemble des actifs numériques en temps réel et permet de lever le doute, de donner l'alerte et d'analyser les tentatives d'attaques. Mais qui possède donc un tel SOC ? A en croire l'intervention du Dr Patrice Guichard, une équipe sécurité bien formée et entrainée constitue une entrée en la matière. Mais pour déployer et faire vivre un véritable SOC il

convient d'aller plus loin et d'augmenter à la fois la vision, la portée et les capacités opérationnelles de cette équipe, et de la doter des moyens de supervision et de corrélation des événements adéquats.
Bien équipés, bien formés, les opérateurs du SOC seront alors à même d'assurer la mission essentielle de surveillance, de gestion des incidents et de remédiation, mais aussi d'apporter leurs expertises variées dans le cadre d'audits divers. Avoir un SOC sous la main est un atout majeur dans la protection contre les cyber-menaces.

Thématique 4 | Threat Intelligence : quand l'intégrer dans sa stratégie de sécurité ?
CTI, pour « Cyber Threat Intelligence ». Ces 3 lettres évoquent immanquablement le Dark Web, les cybermarchés noirs et la cyber criminalité organisée. Qu'en est-il exactement ? La CTI n'a-t-elle vraiment pour seul objectif de parcourir les tréfonds d'internet à la recherche de pirates et d'informations volées ?
Cette présentation remet les pendules à l'heure et reprend de manière factuelle les fondements de la CTI et ses usages. Initialement destinée au secteur bancaire, la CTI apporte maintenant une vision et des capacités d'anticipation aux autres secteurs : le monde industriel ou celui des jeux vidéo ne sont que deux exemples où la CTI permet d'anticiper des attaques de groupes hautement entrainés et efficaces. Et face à de tels adversaires, connaitre leurs agissements, savoir comment ils s'organisent ou encore quels sont leurs armes actuelles se révèle être un atout majeur. La connaissance, c'est le pouvoir !

Thématique 5 | DLP : Quelles bonnes pratiques pour protéger ses données ?
Le DLP, pour « Data Leak Prevention » (prévention des fuites de données), permet aux organisations de mieux contrôler leurs informations sensibles et d'éviter que celles-ci ne quittent l'entreprise à la faveur d'une erreur (le fichier Excel envoyé au mauvais destinataire, par exemple !).
Sur cette table ronde, le Dr Patrice Guichard, ainsi que la représentante de l'ANSI Mme Olfa ENNAR et Mr Amara BOUZAYANI, le DSI de UIB-Société Générale ont abordé aussi bien l'aspect législatif (a-t-on le droit de filtrer ainsi toutes les informations ?), mais bien entendu également technique (le DLP peut être déployé en coupure, en mode filtrant, ou en parallèle, en mode bloquant ou d'alerte simple).
À travers des retours d'expérience concrets, les participants ont montré des cas d'usages du DLP afin d'illustrer tout le champ d'application de ces technologies.

Bonus | Déploiement des solutions ESET, quelle réalité sur le terrain ?
La journée se conclut avec un retour d'expérience majeur : comment déployer 4500 postes en 1 mois et demi sur 350 sites distants, avec une équipe très réduite (une personne en interne et deux jours de prestation externe) ?
C'est l'exploit réalisé par un client ESET, qui partage son expérience en matière d'anticipation, de formation et d'outils, pour arriver à une prise en main rapide de l'outil ESET et une protection élevée.
C'est aussi ici l'occasion pour ESET de rappeler qu'il accompagne les entreprises dans le déploiement, la configuration, l'administration et même la supervision des nouvelles solutions comportementales afin de les aider à en tirer le meilleur parti. Les experts ESET couvrent tout le spectre des besoins, des services à l'externalisation de la cybersécurité à travers des MSSP ou des services managés.
Grâce à ce programme de « Professional Services » ambitieux, ESET et ses partenaires s'allient pour protéger les grandes entreprises !

CONTACT PRESSE :

Darina SANTAMARIA / +33 01 86 27 00 39 / darina.j@eset-nod32.fr
EA Pro Nantes: eapronantes@gmail.com

À propos d'ESET

Fondée en 1992, ESET, 1er éditeur européen en solutions de cybersécurité est spécialisé dans la conception et le développement de logiciels de sécurité pour les entreprises et le grand public (avec respectivement les rangs de 4ème et 5ème mondial). Pionnier en matière de détection proactive des menaces véhiculées par l'Internet, ESET est aujourd'hui le leader dans ce domaine. Il est désigné comme l'unique Challenger dans le Magic Quadrant 2018 de Gartner, catégorie Endpoint Protection Platforms. À ce jour, l'antivirus ESET Nod32 détient le record mondial de récompenses décernées par le laboratoire indépendant Virus Bulletin depuis 1998. Les solutions ESET protègent aujourd'hui plus de 600 millions de postes dans le monde. Pour plus d'informations : **www.eset.com/na/** Blog : www.welivesecurity.com/fr/