Économie de l'insécurité informatique

Malcolm Harkins, Chief Security and Trust Officer, Cylance

CYLANCE

Introduction

Sur le plan de l'économie, le monde de la sécurité informatique est relativement peu performant, ce qui est à la fois une bonne et une mauvaise chose. Une mauvaise chose, parce que des milliards de dollars sont gaspillés sur des solutions qui offrent à leurs acheteurs un rendement inférieur à leurs attentes ; une bonne chose, parce qu'il existe des possibilités de gagner en efficacité et d'améliorer la qualité de vie de chacun.

Le présent document montre que les inefficacités économiques sont parfaitement connues, et explique pourquoi l'industrie ne semble guère disposée à prendre le taureau par les cornes. Lorsqu'elles auront compris ces enjeux, les entreprises seront mieux armées pour choisir des outils efficaces et adaptés à leur mission. Ce livre blanc explique également comment une confiance mal placée peut provoquer des réactions contradictoires du marché.

Quels sont les signes de l'inefficacité économique ?

En économie, l'efficacité se définit comme suit :

> Une situation où chaque ressource est allouée de manière optimale pour servir au mieux chaque individu ou entité, tout en minimisant les gaspillages et les inefficiences[1].

Il convient de noter que le bien-être (ou la qualité de vie) des populations vivant dans une économie donnée dépend directement de l'efficacité avec laquelle les ressources sont allouées. Le niveau d'efficacité maximum est atteint lorsque les ressources disponibles ne peuvent être allouées de manière plus efficace.

Dans cette optique, il est intéressant de se pencher sur l'état actuel de la sécurité informatique. Selon le magazine Forbes, les entreprises investiront environ 93 milliards de dollars dans la sécurité informatique en 2018[2], soit une augmentation de 14 % par rapport aux 71,4 milliards dépensés en 2014[3]. Au cours de cette même période, nous avons été témoins de cyberattaques dévastatrices qui ont notamment touché JPMorgan Chase, Home Depot, Equifax et Yahoo!. Des menaces mondiales comme WannaCry et Petya ont fait les gros titres de la presse, tandis que des cybercriminels particulièrement ambitieux piratait avec succès le réseau électrique ukrainien.

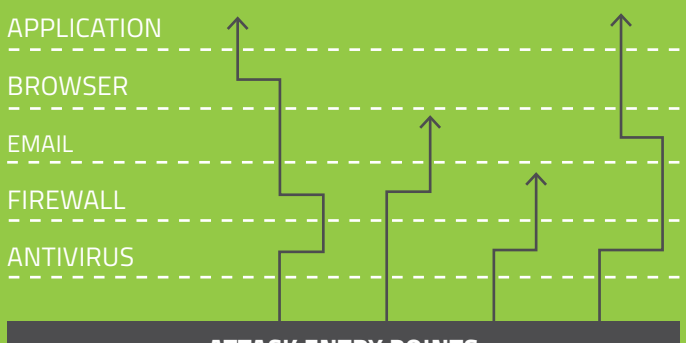
Et vous trouvez que cette industrie garantit une efficacité maximale à ses clients ?

Le Center for Strategic and International Studies suit de près les grands incidents qui frappent le monde numérique depuis 2006. Ses experts définissent une « attaque importante » comme une attaque ciblant « les agences gouvernementales, les entreprises de défense et les sociétés high-tech, ou les crimes économiques entraînant des pertes de plus d'un million de dollars »[4]. Ses recherches indiquent que les cyberattaques importantes ont augmenté de 230 % depuis 2014. En d'autres termes, les entreprises paient 14 % de plus pour mettre fin à un problème qui s'est aggravé de 230 % en quatre ans.

C'est un exemple parfait d'inefficacité économique.

Origines de l'inefficacité

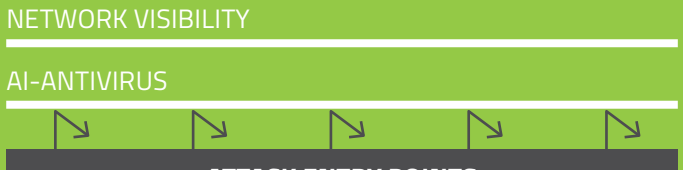
Les racines de l'inefficacité économique se trouvent dans la mauvaise affectation des ressources. Pour comprendre comment le secteur de la sécurité informatique a traditionnellement géré ses ressources en dépit du bon sens, il convient de se demander comment il développe des solutions. Les antivirus et autres produits de sécurité évoluent en adaptant la réponse à de nouvelles menaces, chaque nouvelle solution ajoutant une couche de protection à la précédente.



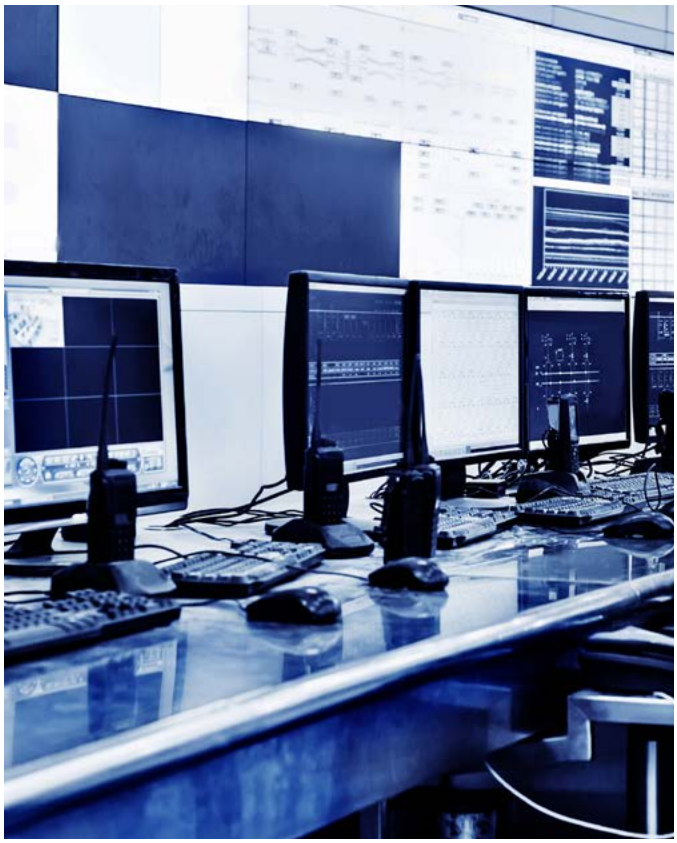
Ancien modèle industriel

Quoique tout à fait compréhensible, cette méthode « réactive » n'est pas vraiment efficace. Chaque couche de protection peut nécessiter des ressources supplémentaires et à terme, la mise en place de nouvelles défenses contre les menaces émergentes alourdit considérablement des solutions de sécurité toujours plus gourmandes en ressources.

Résultat, une inefficacité tout à fait prévisible. Chaque minute consacrée à l'apprentissage de nouveaux systèmes tout comme chaque cycle d'horloge passé à traiter des données de sécurité supplémentaires ne sera pas consacré par l'entreprise à son activité vitale. Les multiples couches de protection basées sur les solutions existantes introduisent de nouveaux conflits dans l'environnement, avec des répercussions directes sur la productivité et, par conséquent, des pertes d'efficacité.



Modèle de prévention Cylance®



À qui profite le crime ?

L'attaque mondiale WannaCry a fait la une des journaux le 12 mai 2017. Trois jours plus tard, Reuters publiait un article intitulé « Cyber security stocks rise in wake of global 'ransomware' attack »[5]. Un mois plus tard, les attaques malveillantes baptisées Petya (plus tard NotPetya) frappaient l'Ukraine avant de se propager dans soixante-quatre autres pays. Le NASDAQ annonce deux jours après la première faille que « les actions en bourse des éditeurs de logiciels de cybersécurité montent en flèche à la suite de l'attaque par ransomware Petya »6. Ces gains profitent à la fois aux éditeurs d'antivirus et aux fonds négociés en bourse (ETF) qui suivent de près le secteur de la sécurité informatique.

Il n'est peut-être pas si étonnant que les éditeurs de logiciels de sécurité profitent des failles de sécurité. L'optimiste supposera que ces hausses des valeurs boursières traduisent un afflux de propriétaires d'entreprises non protégées qui souhaitent sécuriser leurs systèmes à la suite d'une épidémie de malware. Si cette explication peut être recevable cas pour WannaCry en mai 2017, comment alors expliquer que le même phénomène se soit reproduit un mois plus tard avec Petya ?

Une industrie dont l'activité repose sur la fourniture d'outils de sécurité ne devrait pas tirer profit de ces défaillances. Il suffit de penser aux conséquences économiques de l'épidémie de la vache folle. Les éleveurs américains n'ont pas vu le prix du bétail augmenter pour autant. Au contraire, l'industrie bovine américaine a perdu près de 11 milliards de dollars7 sur trois ans. Des pertes considérables enregistrées dans le sillage d'une défaillance publique constituent une réaction courante de la part du marché et ce, que l'entreprise vende des automobiles, des hamburgers ou des smartphones. Si le

« La réactivité qui caractérise les logiciels antivirus existants a abouti à la prolifération de solutions inefficaces. Les entreprises modernes ont besoin de solutions légères et proactives qui se concentrent sur la prévention des failles et non sur des mesures prises après coup. »

secteur de la sécurité informatique constitue à ce titre une exception à la règle, c'est dans une large mesure parce que le grand public lui accorde, à tort, sa confiance.

Une confiance mal placée

La confiance est liée à deux notions fondamentales : la compétence et le caractère. La compétence suscite la confiance en démontrant une certaine aptitude et en produisant des résultats. Le caractère gagne la confiance en affichant intention positive et intégrité. Le grand public fait confiance aux éditeurs de logiciels de sécurité informatique pour le protéger contre les logiciels malveillants. C'est ce qui ressort clairement de la réaction positive du marché dont les entreprises éditeurs d'antivirus bénéficient lors de l'apparition de malware d'envergure mondiale. Mais cette confiance est-elle réellement méritée ?

Compétence — Il est difficile de prétendre que la sécurité informatique a gagné en compétences au fil du temps avec, d'année en année, des failles de sécurité qui semblent toujours plus graves. En réaction, les utilisateurs versent toujours plus d'argent à un secteur qui peine à les protéger, les éditeurs d'antivirus proposant en retour une palette de plus en plus large de nouveaux produits ou services. Ces solutions installées après coup peuvent s'avérer plus onéreuses pour l'environnement informatique et ajouter des points de conflits.

Caractère — Le commentaire ci-dessous concernant les failles de sécurité a été prononcé en mai 2017 lors d'une rencontre entre responsables de la sécurité des systèmes d'information (RSSI) à Los Angeles :

> « Il faut l'accepter.... ils vont y venir. »

Malheureusement, cette déclaration reflète un avis solidement ancré chez de nombreux experts en sécurité informatique. Pourtant, leur objectif n'est pas de réduire les intrusions, mais de les endiguer. Il est dès lors légitime de s'interroger sur la véritable intention d'entreprises qui partent du principe que les cybermenaces ne peuvent être stoppées.

Aligner les objectifs

Les entreprises doivent s'assurer que les objectifs de leur fournisseur de logiciels de sécurité correspondent aux leurs. Est-ce que les éditeurs d'antivirus professionnels se soucient réellement de la performance globale de leurs clients ? Ou les

poussent-ils à acquérir des rustines multicouches inefficaces tout en sachant que les failles sont inéluctables ?

La nature réactive des antivirus a jusqu'à présent abouti à la prolifération de solutions inefficaces. Aujourd'hui, les entreprises ont besoin de solutions légères et proactives qui mettent l'accent sur la prévention des failles, et non sur une réaction a postériori.

En d'autres termes, l'ancien modèle de la sécurité informatique a pour objectif de vendre aux entreprises des camions de pompier, des tuyaux, des prises d'eau et des échelles en cas d'incendie criminel, alors qu'un fournisseur dont les objectifs sont alignés sur les vôtres proposera une solution davantage proactive et moins gourmande en ressources. Par exemple, en utilisant des matériaux de construction ignifuges, en l'implantant dans un quartier sûr et en installant des capteurs pour qu'aucun criminel ne pénètre sur le site sans être détecté.

Conclusion

La nature « réactive » de la sécurité informatique a favorisé la création de solutions multicouches qui brillent par leur piètre efficacité. Les éditeurs d'applications de sécurité ont adopté une philosophie selon laquelle les failles de données sont inévitables, favorisant ainsi une culture alliant médiocrité et apathie. La confiance mal placée du public permet aux éditeurs d'antivirus de manquer à leurs devoirs tout en évitant les inconvénients liés aux forces du marché. En résumé, les entreprises de sécurité informatique profitent de la situation et n'ont guère d'intérêt à ce qu'elle change.

L'avenir de la sécurité informatique passe par l'adoption de solutions proactives, préventives et légères qui correspondent à la mission professionnelle des acheteurs. Ces solutions doivent introduire un minimum de conflits dans l'environnement informatique en visant une prévention totale des menaces, et non en ajoutant sans cesse une nouvelle défense sur les ruines de la précédente.

Depuis quatre ans, le secteur de la sécurité informatique a augmenté ses tarifs tandis que ses performances se dégradaient. Tant que le marché n'aura pas changé sa vision de l'industrie de la sécurité, cette tendance aura de beaux jours devant elle.

À propos de Cylance

Cylance utilise l'intelligence artificielle pour fournir des produits et des services de sécurité prédictive spécialisés et focalisés sur la prévention, qui modifient la façon dont les entreprises abordent la sécurité de leurs postes de travail et de leurs serveurs. Les solutions de sécurité de Cylance assurent une prévention prédictive d'un large spectre de menaces avec une visibilité panoramique de l'entreprise, combattant des menaces telles que les logiciels malveillants, les rançongiciels, les attaques sans fichiers, les scripts malveillants, les documents militarisés et autres vecteurs d'attaque. Grâce à la prévention des logiciels malveillants, au contrôle des applications et des scripts, à la protection de la mémoire, à la mise en œuvre de règles concernant les périphériques, à l'analyse des causes profondes, à la traque des menaces, à la détection des menaces avec réponse automatisée, que complètent des services de sécurité spécialisés basés sur l'intelligence artificielle, Cylance protège les postes de travail et les serveurs sans augmenter la charge de travail des utilisateurs ni les coûts, tout en assurant une sécurité maximale et un retour sur investissement continu.

Endnotes

[1] Economic Efficiency, (Investopedia, 2018)

[2] Gartner Predicts Information Security Spending To Reach $93 Billion In 2018, (Forbes, 2017)

[3] Cybersecurity Market Reaches $75 Billion In 2015; Expected To Reach $170 Billion By 2020, (Forbes, 2015)

[4] Significant Cyber Incidents, (CSIS, 2018)

[5] Cyber security stocks rise in wake of global 'ransomware' attack, (Reuters, 2017)

[6] Cybersecurity Stocks Shoot Up on Petya Ransomware Attack, (NASDAQ, 2017)

[7] Mad-cow ban cost U.S. $11 billion in beef exports, (Reuters 2008)

+33-1-86261825
sales@cylance.com
www.cylance.com/fr
4 place de l'Opéra, 75002 Paris, France

20180710-0815