Sécurité : 15 ans d'échec

Jonathan Brossard

Dans Sécurité et stratégie 2012/4 (11), pages 6 à 14
Éditions Club des Directeurs de Sécurité des Entreprises

ISSN 2101-4736
DOI 10.3917/sestr.011.0006

Sécurité : 15 ans d'échec

Jonathan Brossard

Rares sont les témoignages livrés *in vivo* et sans retenue sur un sujet aussi sensible que la sécurité informatique. Dans un récit qui n'épargne personne, Jonathan Brossard livre son expérience de hacker, chercheur en sécurité, et présente un tableau d'ensemble sans concession. Après une quinzaine d'années d'existence, quelques vérités expérimentales s'imposent quant à la sécurité de l'information sur Internet : « *ça coûte cher, ça marche mal, et le futur prédictible ressemble à un vaste salmigondi de technologies non maîtrisées, de logiciels maison jamais réellement maintenus et de dissolution dans le « cloud » de la ligne maginot qu'incarnait le « mur par feu » de l'entreprise entre un Internet barbare et un Intranet se voulant sécurisé* ». Voici en substance le constat d'échec dressé par l'auteur et expliqué sous forme de témoignage personnel dans cet article.

J'ai eu la chance de participer en tant qu'expert en sécurité à certains projets d'ampleur conséquente. Ces dernières années, j'ai par exemple aidé une Banque du Commonwealth à moderniser son réseau informatique dans le cadre d'un projet quinquennal à raison d'un milliard USD par an. Je fais également partie des quelques chercheurs français qui participent à la communauté internationale de la sécurité informatique, en présentant les recherches effectuées au sein de mon entreprise Toucan System via des conférences organisées dans le monde entier sur la sécurité informatique. Ces derniers mois, j'ai eu le plaisir d'être invité à présenter mes recherches sur la sécurité du BIOS aux conférences du Chaos Computer Club en Allemagne, ou encore BlackHat et Defcon aux Etats-Unis. J'ai enfin permis de corriger des bugs dans des logiciels complexes tels que Bitlocker (Microsoft), Truecrypt, McAfee Endpoint ou encore Adobe Reader... et bon nombre d'antivirus du marché. Fort de ces expériences, je me risque dans le présent essai à quelques réflexions personnelles sur l'état de la sécurité informatique, en tentant non pas de torpiller telle ou telle technologie, mais en cherchant à expliquer pourquoi fondamentalement, il est des approches qui ne peuvent pas fonctionner... même si elles se vendent bien !

Mise à nue de logiciels inopérants

Si l'on en croit les chiffres avancés par Jeremiah Grossman à la conférence Shakacon 2012 à Hawaï, nous, en tant qu'entreprises utilisant Internet de par le monde, dépensons collectivement 8 500 000 000 USD par an en antivirus, Systèmes de Détection d'Intrusion (IDS) et firewalls, et 500 000 000 USD en « tests d'intrusion ». D'un point de vue pratique, on entend par là le recours aux « scans », cherchant à déterminer si

un système comporte certaines vulnérabilités connues.

Les résultats, on ne peut le nier, ne sont pas à la hauteur, non pas des attentes, mais plus fondamentalement des besoins. Quel Etat, quelle entreprise au monde peut se vanter en effet d'être à l'abri des attaques informatiques quand les médias font état d'intrusions de grande ampleur et sur de longues durées au sein des entreprises censées être les mieux préparées, et ce, de manière fort régulière ?

> **La taille d'un seul processus dans la mémoire d'un simple ordinateur de bureau équivaut à 2 puissance 64 bits. Soit la même quantité que l'ADN sur DVD « au carré ».**

En guise de précaution oratoire, on rappellera que les problèmes liés à la vulnérabilité des systèmes d'information sur Internet sont essentiellement d'ordre logiciels, et que, ce faisant, ils sont généralement d'une complexité titanesque. Qu'on juge plutôt : l'ADN d'un être humain exprimé en bit d'information (0 ou 1), comprend l'équivalent d'un DVD d'information, soit 2 puissance 32 bits. La taille d'un seul processus dans la mémoire d'un simple ordinateur de bureau équivaut à 2 puissance 64 bits. Soit la même quantité que l'ADN sur DVD « au carré ». Et contrairement à celui-ci, le processus est dynamique, à raison de milliards d'opérations par seconde qui modifient ses informations (typiquement les données et le code). Il évolue dans le temps pour charger des modules ou entre les versions du même logiciel bien sur, mais jusqu'entre chaque lancement du même programme dans la même version sur la même machine en fonction des mêmes paramètres d'entrée ! Or, un processus est interdépendant du noyau, d'autres processus, ou d'autres machines... Une vulnérabilité typique consistera par exemple, au niveau le plus élémentaire de l'instruction du microprocesseur, dans le fait de ne pas écrire l'information au bon endroit, de ne pas écrire la bonne quantité de données de quelques octets, ou de confondre l'état de deux adresses mémoire.

Pour remédier à ce type de vulnérabilité, on pourrait arguer que l'on va « prendre de la hauteur », agréger les données, utiliser une représentation intermédiaire ou encore prendre les vulnérabilités dans leur globalité, etc. Rien n'y fait. D'un point de vue pratique, le niveau de granularité où s'identifie, s'exploite ou se corrige (ou pas) une vulnérabilité, n'est pas 1 bit, mais 8 bits (soit 1 octet d'information) puisqu'il s'agit de la taille élémentaire à laquelle les microprocesseurs traitent l'information. Si vous cherchez « plus haut », votre résolution visuelle est trop faible pour appréhender la complexité du problème ! Diantre !

La réalité est que l'espèce humaine ne sait finalement que très peu de choses sur le fonctionnement de machines qui nous sont devenues, n'ayons pas peur de l'originalité, essentielles. Nous savons bien entendu les fabriquer et faire fonctionner des programmes dessus, mais quant à prédire leur comportement, et *a fortiori* leur sécurité, quasiment rien ne peut être démontré analytiquement.

A la lecture de mon diagnostic à charge, vous devez vous dire que j'exagère. Je vous concède que l'on sait tout de même prouver une chose : « *il est impossible d'écrire un logiciel qui prédit si un autre programme va s'arrêter* », ainsi que l'a énoncé Alan Turing. Il n'y a alors qu'un pas pour prouver que l'on peut provoquer à l'intérieur du même programme un « *heapoverflow* » (un débordement de données sur un espace mémoire alloué, pouvant mener au détournement de la fonction d'un programme), une collision cryptographique ou une

anomalie dans une fonction d'authentification... Sur le plan de la sécurité, cela semble, avouons-le, mal engagé !

De ce point de vue, les 8,5 milliards évoqués précédemment sont dépensés essentiellement en outils qui sont, il est bon de le rappeler, eux-mêmes des logiciels dont on ne sait donc pas davantage prévoir le comportement. La plupart est, sous une forme ou sous une autre, un moyen de filtrer de l'information (« un parser »). Dans l'écrasante majorité des cas, pour avoir une utilité quelconque, il est impératif d'avoir des fameuses « mises à jour » de signatures associées aux dits filtres. Il peut s'agir de signatures d'antivirus, de signatures d'attaques pour de l'inspection de paquets ou d'un pare-feu applicatif, ou bien encore du filtrage de flux dangereux. En d'autres termes, nous tentons par ces « mises à jour » de réduire l'espace des vulnérabilités possibles à celles qui sont déjà connues.

En 1999, lorsqu'Internet produisait moins de 10 000 virus par an, il était permis de croire possible un recensement exhaustif de ces virus. En 2012, le même nombre est produit chaque jour alors que dans le même temps, les antivirus sont de moins en moins performants. J'en veux pour preuve le fait que même les entreprises dotées d'antivirus sont tout de même victimes d'infections. Dans la même logique, les logiciels d'audit automatisé des vulnérabilités fonctionnaient raisonnablement en 2000 lorsqu'Internet publiait une dizaine de vulnérabilités intéressantes par an. Ils n'ont plus grand intérêt en 2012 quand des douzaines de vulnérabilités sont publiées chaque jour puisqu'il n'est pas possible d'écrire autant de tests, d'autant que les vulnérabilités les plus critiques sont désormais d'une part bien plus complexes qu'au tournant du siècle. Leur moyen de détection traduit encore davantage la faiblesse des logiciels d'audit puisqu'elles sont de plus en plus découvertes « dans la nature », c'est à dire une fois que les attaquants en on fait un virus qui se propage hors de tout contrôle, ou à la suite d'une utilisation excessive qui aurait attiré l'attention d'un utilisateur ou d'un administrateur réseau se donnant la peine d'isoler le binaire et de l'envoyer à un éditeur d'antivirus.

Enfin, les « tests d'intrusion » qui consistent à vérifier, en général à l'aide d'outils largement automatisés, si certaines vulnérabilités connues sont présentes sur un logiciel ou une infrastructure donnée, sont du même acabit. Personne n'est dupe sur leur exhaustivité ou sur leur efficacité. Pensez-vous vraiment que Sony, Google ou Microsoft n'ont jamais fait « pentester » (réaliser des tests d'intrusion) leurs infrastructures ou leurs sites web avant d'être victimes d'intrusions ? La réalité est que les vulnérabilités que ces outils sont capables de détecter ne représentent qu'une infirme portion des vulnérabilités effectivement présentes dans les logiciels audités.

Quand les attaques sont ciblées, c'est-à-dire que du code a été écrit sur mesure pour détecter et exploiter une vulnérabilité sur vos systèmes, la prévention offerte par ces outils est nulle. Les antivirus ne savent ni détecter ni, *a fortiori*, prévenir une corruption mémoire. Le filtrage par *firewall,* même avec authentification, filtrage applicatif et pourquoi pas chiffrement, est totalement inutile en l'état de l'art des techniques d'exploitation. On pourra par exemple lire à ce sujet le récent *shellcode* implémentant une session utilisateur vers Internet, à travers un proxy applicatif https avec authentification sous Windows publié dans l'outil Metasploit.

Pour ce qui est du code « maison », il s'agit en général d'un code, certes, non public, mais maintenu à minima, et sans support ou audit technique vraiment poussé. Les entreprises utilisent souvent du code que personne ne comprend. Dans le meilleur des cas, la documentation tech-

nique à disposition est déraisonnable, un humain ne pouvant pas assimiler plusieurs milliers de pages en deux jours par exemple. Surtout : les vulnérabilités que l'on ne connaît pas (0-days) ne sont, on me pardonnera cette lapalissade, pas documentées. Or, sans documentation, le nombre de personnes dans l'entreprise capables de comprendre les nouvelles propriétés des logiciels chute. En outre, si le code source n'est pas disponible, ce qui est fréquemment le cas, plus personne ne sait faire. L'ingénierie inverse, à savoir l'analyse dynamique de binaires ou l'analyse statique de listings en assembleurs, n'est pas encore arrivée dans les entreprises.

> **Le problème de la sécurité de l'information ne trouvera pas de solution significative à coups d'antivirus, de firewall ou d'IDS.**

Il convient d'être intellectuellement honnête sur un point : le problème de la sécurité de l'information ne trouvera pas de solution significative à coups d'antivirus, de firewall ou d'IDS (Intrusion Detection System). Au mieux, ces derniers ont pour utilité relative de produire un effet contre le « bruit de fond ». En clair, ils vont empêcher que vous soyez contaminé par une attaque qui ne vous ciblait pas (exempligratia : propagation de vers, scripts automatisés scannant tout Internet). C'est là autant d'économies réalisées en temps de maintenance et en disponibilité du réseau, des serveurs et des postes de travail, mais cela n'a pratiquement aucune utilité contre une attaque ciblée ou utilisant un « exploit 0-day », c'est-à-dire un code exploitant une vulnérabilité non connue (ni par le vendeur du dit logiciel, ni par aucun antivirus, et donc pour ainsi dire personne).

Par ailleurs, un firewall, même avec authentification, un proxy applicatif, ou bien encore une séparation totale du DNS, ne vous protège pas contre un exploit développé sur mesure pour vous attaquer et n'empêche pas un attaquant de contrôler à distance une machine ou d'exfiltrer des documents vers Internet. Un IDS ou un IPS (Intrusion Prevention System) qui prétend effectuer un « deeppacket inspection » (DPI) réimplémente des couches applicatives pour prétendument détecter des vulnérabilités dans les mêmes couches applicatives. Ils sont donc vulnérables aux mêmes problématiques d'implémentation ! Ainsi, ces IDS commerciaux populaires utilisent les librairies de compression zlib pour détecter des exploits dans les librairies zlib... du pain béni pour un attaquant ! Pour ahurissant que cela puisse paraître, ces solutions se vendent pourtant.

L'inefficacité d'une protection qui ne détecte ni les « 0-days », ni les attaques ciblées pose un sérieux problème lorsque l'on sait, d'après Grossman que le coût cumulé de ces solutions de sécurité représente l'intégralité ou peu s'en faut du budget sécurité des entreprises. Par conséquent, il convient de se demander si les entreprises ne sont pas tout simplement surprotégées contre les attaques de type « bruit d'Internet » ? Pour comparaison, une récente étude de chercheurs anglais estimait que l'un des plus importants botnet du monde, émetteur d'une partie tout à fait significative du spam mondial, rapportait autour de 3 millions d'euros par an à son propriétaire. Les chercheurs en ont conclu à un facteur de l'ordre de 1000 entre le budget mondial de la sécurité informatique et celui de la menace !

Des politiques de sécurité d'entreprise inadaptées et inefficaces

Par ailleurs, les projets que les entreprises entendent mener à bien en matière de technologies d'information et de communication ne sont-ils

pas d'une complexité démentielle ? Dans une entreprise donnée, qui comprend vraiment ce qu'est par exemple la virtualisation ? Non pas en théorie ou d'après les manuels utilisateurs, mais via la maîtrise des détails d'implémentation de A à Z en passant par VT-X ? Pour le niveau qui nous intéresse (8 bits donc), personne ne comprend probablement aucun logiciel de taille même petite dans son intégralité. Mettons qu'une ligne de C représente environ cinq instructions assembleur. Un noyau typique a des millions de ligne de C. En comptant ne serait-ce qu'un million de lignes, on cherche des vulnérabilités de l'ordre de une ligne. Sur un corpus de 833 livres de 200 pages chacun. Et le code change à chaque mise à jour...

Pour mener à bien les dits projets, les plus grosses entreprises peuvent se permettre de faire appel à des équipes conséquentes de designers et architectes informatiques. Mes échanges avec ces derniers sont souvent enrichissants, leur passion pour leur métier étant stimulante. Cependant, je ne peux qu'être inquiet quand je constate le manque de culture générale de ces derniers lorsqu'il s'agit de sécurité informatique, et ce, quelle que soit l'entreprise concernée. Pour dire les choses avec une once de cruauté, il ne me paraît guère possible de dessiner un réseau informatique lorsque l'on ne sait pas coder. Or, vous seriez surpris de constater que la plupart des architectes réseaux ne savent en réalité pas écrire de code !

A l'heure où l'Estonie introduit la programmation en C et Python dans ses programmes éducatifs dès l'école primaire, n'est-il pas temps de nous poser nous aussi la question de l'acquisition de ces savoirs fondamentaux par le plus grand nombre ? Si l'on accepte le fait qu'Internet n'est pas un simple phénomène de mode, mais bel et bien le nerf de l'information mondiale pour les décennies à venir, n'est-il pas urgent de combler nos lacunes en termes de savoirs informatiques fondamentaux ?

A ce jour en France on déplore l'absence de politique volontariste, un enjeu vital auquel les gouvernements successifs n'ont pas suffisamment donné d'importance alors que nous vivons la troisième révolution industrielle ; son point de départ est daté de 1971 lorsque Intel met sur le marché le premier microprocesseur. J'aime à croire que dans 10 ans, les fondamentaux pédagogiques s'articuleront autour du triptyque : « savoir lire, savoir écrire, savoir écrire du code ». De fait, la compréhension de la chose informatique change absolument radicalement le jour où vous apprenez à parler à un ordinateur, non pas au travers d'un logiciel écrit pas un tiers, mais par vous-même. On pourrait penser que savoir utiliser un logiciel de messagerie mail et un navigateur web constitue le bagage essentiel pour travailler en entreprise en 2012. Sauf que si vous ne comprenez pas comment ces derniers fonctionnent, il est impossible d'assurer votre sécurité. Le nombre d'exploits « coté client » dans ces logiciels ainsi que dans les suites bureautique de base ont eu raison du modèle ancestral de la sécurité, à savoir : le firewall délimite la frontière entre les gentils et les méchants. Vu la facilité à pénétrer un réseau en envoyant un pdf piégé à un département de l'entreprise n'ayant pas *a priori* une connaissance fine de l'informatique (notamment le département ressources humaines), il serait utile à mon sens d'obliger un maximum d'employés, non pas à suivre des formations dédiées à la sécurité, mais à développer leur maîtrise fondamentale de l'outil informatique. Si je n'ai aucune illusion sur le fait que les travailleurs actifs ne feront pas cet effort au cours de leur vie professionnelle, je crois en revanche que les jeunes générations le feront. Du coup, j'anticipe d'ici 10 ans une dichotomie entre des jeunes capables de maîtriser non plus seulement l'usage pratique d'un pc, mais également le développement de logiciels, et leurs aînés, proprement

illettrés de l'ère numérique, et qui concentreront l'essentiel du risque informatique de l'entreprise.

On ne peut envisager la sécurité d'un réseau sans en comprendre l'historique dans son ensemble. Or en 2012, le principal problème d'un réseau informatique d'une entreprise de taille conséquente (mettons, plus de 1000 personnes) est sans conteste la gestion de ce que les Anglo-saxons nomment la « legacy ». De fait, si vous choisissez aujourd'hui d'opter pour telle ou telle technologie, vous êtes mariés avec la dite technologie pour les 10 ou 20 ans qui viennent. Ce qui implique d'envisager la maintenance et la sécurité de ces technologies sur cette période. Force est de constater qu'il y a 10 ou 20 ans, cette vision des choses ne prédominait pas. Nous sommes aujourd'hui héritiers de cette vision à court terme, ce qui explique par exemple la part de marché incroyable de Windows XP en entreprise. De fait, même si ce système d'exploitation sorti en 2001 a presque 15 ans en termes de design, il représente toujours 40% du marché, essentiellement d'ailleurs dans les entreprises. La raison en est simple: beaucoup d'entreprises ne peuvent tout simplement pas migrer vers des plateformes ultérieures sans dans le même temps se passer d'applications critiques qui ne sont plus maintenues ou plus compatibles ! Or, je vous ferai grâce de toutes les améliorations dont tout système d'exploitation a bénéficié durant la dernière décennie, mais il n'est pas de doute permis quant au fait qu'un système d'exploitation 64 bits s'exécutant sur un microprocesseur supportant la non-exécution de pages mémoire (le bit « NX »), dont l'allocation dynamique de mémoire est protégée (« safeunlinking »), l'adressage rendu aléatoire (« ASLR ») et l'intégralité du code soumis à des analyses statiques et dynamiques systématiques tel que c'est le cas pour Windows 7 ou 8 est d'un niveau de sécurité incomparable avec celui d'un système d'exploitation comme XP. Bien des entreprises me demandent d'ailleurs comment être à la pointe de la sécurité tout en demeurant sous XP pour des raisons de compatibilité. La réponse est bien simple: vous ne pouvez pas. Point.

Bien des entreprises me demandent d'ailleurs comment être à la pointe de la sécurité tout en demeurant sous XP pour des raisons de compatibilité. La réponse est bien simple: vous ne pouvez pas.

Dans le même ordre d'idées, il est fréquent d'entendre un RSSI comparer la sécurité de son réseau à hauteur des investissements réalisés à cette fin, par rapport à ses concurrents. C'est ma foi le plus mauvais *benchmark* possible; eux aussi sont complètement dépassés par la situation; le vrai *benchmark* pertinent serait de comparer un budget sécurité à celui des attaquants ! Or, si les vendeurs rabâchent des chiffres invérifiables et alarmistes quant aux APT (« advanced persistant threats », c'est-à-dire des menaces durables et largement opportunistes), CPT (« Chinese persistant threats ») et autres cyber-guerres, il est un chiffre vérifiable quant à la menace informatique : le budget que les Etats allouent à la sécurité informatique offensive. Je suis de ceux qui pensent que la menace principale pour une grosse entreprise vient en effet d'une attaque émanant d'un Etat, et pas de groupes d'adolescents isolés ou d'hacktivistes patentés: ces derniers jouent dans la catégorie « petits joueurs », même si Lulzsec, Antisec ou Anonymous ont démontré qu'ils pouvaient mettre à mal ponctuellement la sécurité de peu ou prou n'importe quelle entreprise. Or, si l'on s'arrête un instant sur les capacités offensives allouées ici et là par les Etats, il est clair que les deux dernières années ont constitué un tournant dans l'histoire de la sécurité informatique. Ainsi en est-il de la NSA qui, avec son *Data Center* dans

l'Utah, prévoit d'enregistrer ni plus ni moins que l'intégralité du trafic circulant sur le Net. On pourrait trouver la chose ridicule s'agissant de trafic chiffré par des algorithmes forts tels que SSL et RSA. Sauf que la NSA investit également massivement dans les universités américaines (Princeton) et étrangères à la pointe des ordinateurs quantiques, qui peuvent déjà factoriser des nombres premiers (IBM a réussi l'an dernier à factoriser le nombre 15=5*3 sur un module quantique dédié) : il est tout à fait réaliste de penser que d'ici cinq ans, ils sauront factoriser un nombre sur 1024 bits, et ainsi déchiffrer toutes les données accumulées durant des années. Entreprises, votre risque est celui-ci. Côté Français, on assiste actuellement à un curieux chamboulement, avec la création de l'ANSSI tout d'abord. Leurs intentions défensives me semblent tout à fait discutables étant donné leur recrutement massif de tous les experts en sécurité offensive disponibles dans l'hexagone, avec pour effet de bord la véritable spoliation du savoir dans le secteur privé : si ma start-up n'a eu à déplorer aucun départ pour l'ANSSI, tel n'est pas le cas du reste des cabinets de conseil en sécurité informatique, où l'ANSSI a opéré des recrutements massifs. Je tiens à les remercier pour ce coup de pouce inattendu...

Les experts en sécurité sont assez d'accord sur le fait que les Etats sont les premiers acheteurs d'exploits sur le marché noir, et utilisent ces derniers pour gagner des marchés bien plus qu'ils ne le font pour contrecarrer les plans de terroristes ou de pédophiles.

On me répondra que l'ANSSI, tout comme la NSA, se focalise sur la défense des infrastructures critiques. Il s'agit au mieux d'une bonne blague. Les capacités offensives servent avant tout à faire gagner des contrats et partant des parts de marchés aux entreprises nationales. Je ne me risquerai pas à donner d'exemples afin de ne pas encourir de procès en diffamation, mais les experts en sécurité sont assez d'accord sur le fait que les Etats sont les premiers acheteurs d'exploits sur le marché noir, et utilisent ces derniers pour gagner des marchés bien plus qu'ils ne le font pour contrecarrer les plans de terroristes ou de pédophiles. Je ne vends moi-même pas d'exploits à qui que ce soit, malgré des demandes insistantes et répétées, et ce, pour des raisons éthiques évidentes. En revanche, en tant que chercheur, je suis en contact permanent avec des individus moins scrupuleux. Je peux sans risque vous affirmer que ce qui se vend sur le marché noir sert bien plus à pirater des entreprises ou des Etats, que des terroristes et des particuliers. Il est en tout cas de notoriété publique que, dans les années 1970, la NSA a favorisé DES qu'ils savaient casser comme standard de chiffrement américain (« AES », pour « American Encryption Standard »). Il est tout aussi connu que la France a délibérément choisi de diminuer le niveau de sécurité du standard du protocole GSM, en décidant d'imposer un chiffrement 56bits... dont les 10 premiers bits sont à 0 d'après le standard ! Sur un plan plus pratique, Karsten Nohl s'est chargé de montrer que le protocole GSM n'offre absolument aucune sécurité en déchiffrant tout d'abord des trames GSM, puis en clonant purement et simplement un téléphone mobile à la dernière conférence du CCC (Allemagne). Si la compétence des entreprises stagne depuis une dizaine d'années, celle des hackers « underground » atteint des niveaux sans précédent (tout simplement parce qu'ils accumulent de l'expérience) au point de rivaliser avec les meilleurs équipes de R&D des vendeurs, et celle des Etats explose littéralement, en raison des budgets alloués (le budget prévisionnel du *Data Center* de la NSA est estimé à 2 milliards USD) et de la concentration des meilleurs experts nationaux en leur sein.

Encore une réflexion sur le cas français. De par notre culture élitiste du diplôme et le respect à outrance de la hiérarchie, nous nous coupons de la majeure partie de nos talents en sécurité informatique. Un expert en sécurité a moins de 40 ans (d'ailleurs je ne connais pas un seul expert majeur de plus de 40 ans sur la planète). Il n'a souvent pas de diplôme pour la simple et bonne raison que l'enseignement en sécurité est au mieux balbutiant, en réalité inexistant pour ce qui est de former non pas des individus quelque peu au fait des dernières nouveautés en matière de sécurité, mais des chercheurs capables de s'adapter à des technologies qu'ils n'ont jamais côtoyées. L'essentiel des meilleurs chercheurs français travaille ainsi à l'étranger, de chez Google en Californie jusqu'au siège de Microsoft à Redmond, en passant par plusieurs start-ups, de Londres à Brisbane en passant par Bangkok, où leurs qualités techniques sont bien plus reconnues et leur impact sur l'informatique mondiale décuplé. Tant mieux pour eux, mais tant pis pour nous (en tant que Français).

l'architecture d'un pc est par nature impossible à sécuriser d'une modification par la « supply-chain » : nos chers pc ont une architecture datant des années 1980, et dont on ne peut pas assurer l'intégrité !

Pour parachever ce triste tableau, je vais vous faire une confession. Je vous ai menti. Les vulnérabilités matérielles existent. Elles sont mêmes très recherchées parce qu'elles sont fondamentales (elles affectent tout le monde) et ne sont peu ou prou jamais réparées. Leur coût serait tout simplement exorbitant. Du point de vue d'un attaquant, elles sont donc particulièrement intéressantes parce que non seulement elles affectent souvent tous les systèmes d'exploitation, mais encore parce que bien que plus fondamentales, elles ne seront jamais « patchées ». La dernière conférence BlackHat a connu son lot de vulnérabilités très bas niveau. Ainsi Rafal Wojniak a-t-il découvert qu'une instruction des processeurs Amd avait un comportement différent de leurs cousins Intel. Bilan : il a ainsi réussi à exploiter une nouvelle classe de vulnérabilités sur Windows, Linux, BSD (augmentation locale de privilèges) et même Xen (sortie de l'hyperviseur!). Felix Lindler s'est quant à lui attaché à étudier le fonctionnement d'un routeur Huawei à la conférence Blackhat : ses conclusions quant à la qualité de l'architecture et de la couche logicielle sont implacables : ces routeurs sont impossibles à sécuriser. Pour ma part, j'ai tenté de démontrer que l'architecture d'un pc est par nature impossible à sécuriser d'une modification par la « supplychain » : nos chers pc ont une architecture datant des années 1980, et dont on ne peut pas assurer l'intégrité ! Si un fournisseur s'amusait à placer une *backdoor* sur un *firmware* d'une carte mère de pc (soit en modifiant le BIOS, soit en flashant un *firmware* PCI), il pourrait ainsi *backdoorer* un pc d'entreprise de manière indétectable pour tout logiciel (antivirus, etc) et permanente (la *backdoor* n'est pas sur le disque dur). Il n'y a pas de patch possible, il va falloir vivre avec...

Sans aller jusque-là, le choix par les entreprises de leurs fournisseurs semble parfaitement décorélé de toute considération de sécurité, et ce, au profit d'une part des leaders du marché, même s'ils sont objectivement mauvais, et de certaines modes lancées auprès du grand public par des individus parfaitement incompétents, mais qui font loi. Oracle est une illustration du premier phénomène : qu'une vulnérabilité critique (la vulnérabilité « TNS listener ») leur ait par exemple été rapportée en 2008 pour n'être finalement patchée qu'en 2012 au mépris complet de la sécurité de leurs clients n'étant pas suffisant,

Oracle a encore choisi de ne corriger que la future version de leur base de données, laissant tous leurs clients existant vulnérables. Je constate pourtant peu de migrations d'Oracle vers des solutions alternatives en entreprise. A tel point qu'il est une vérité empirique sidérante : la plus mauvaise solution technique remporte toujours le marché. Ainsi en est-il par exemple de MS DOS (au nom de code QDOS, pour « Quick and Dirty Operating System », c'est-à-dire « Système d'exploitation vite fait, mal fait »), qui n'arrivait pas à la cheville d'un système tel que BSD en 1980. Le BYOD (« Bring Your Own Device »), c'est-à-dire le fait d'intégrer des tablettes et smartphones personnels des employés au réseau d'une entreprise, illustre assez bien la seconde tendance. C'est en effet un non-sens complet : non seulement ceci ne se justifie pas par le coût des appareils en question (dérisoire rapporté au budget informatique d'une entreprise), mais en terme de traçabilité de l'information, cela revient à inclure dans le périmètre de sécurité de l'entreprise les appareils et même le réseau des particuliers. Effet carnage garanti.

En guise de conclusion, je me permettrai une prophétie. Je crois que d'ici 10 ans, un réseau d'entreprise ne ressemblera pas à un réseau domestique tel que c'est encore très largement le cas aujourd'hui. De fait, l'architecture « pc uniforme » atteint ses limites : soit l'on ferme les architectures, tel que pressenti sous Windows 8, pour en faire une architecture inadaptée au besoin des particuliers (imaginez-vous réellement devoir déchiffrer puis rechiffrer tout votre disque dur pour pouvoir changer un périphérique défectueux, par exemple un lecteur de dvd, comme c'est le cas avec Bitlocker sous Windows 8 !), soit on l'ouvre au risque de limiter sévèrement la possibilité de traçabilité de l'information, primordiale en entreprise. J'aime à croire que même si le coût en sera certain tant pour les fabricants de matériels que pour les éditeurs de logiciels, il s'agit de la seule option possible. Par ailleurs, puisque le seul avantage compétitif durable est la capacité à apprendre, j'invite cordialement mon aimable lectorat à participer à une prochaine conférence que je coorganiserai et qui rassemblera l'an prochain quelques-uns des meilleurs chercheurs de la planète à Paris afin d'échanger, sans interférence des vendeurs, sur le thème de la sécurité. ■

Jonathan Brossard, hacker, chercheur en sécurité.