Alain Bouillé, Cesin : « WannaCry doit pousser les entreprises à patcher plus vite »

Silicon.fr : Comment le Cesin et ses adhérents ont-ils traversé la crise WannaCry ?

Alain Bouillé : A partir du vendredi, où les RSSI ont commencé à recevoir des alertes sur le type de malware auquel nous allions faire face et sur sa virulence, la communauté des responsables de la sécurité des systèmes d'information s'est mobilisée à des degrés divers, en fonction du niveau d'application des patchs Microsoft diffusés en avril. Les entreprises qui avaient largement appliqué ces correctifs se sont contentées d'une vérification, ce qui leur a permis de découvrir qu'il y avait encore des lacunes à combler. Les plus exposées ont été confrontées à une vraie crise. Elles ont patché dans l'urgence là où, d'habitude, elles mettent beaucoup de temps pour ce faire. Dans un cas comme celui de WannaCry, il faut faire des choix. D'habitude, appliquer les patchs de sécurité revient à se protéger d'un risque faible au prix d'une prise de risque non négligeable sur la continuité des systèmes. Désormais, on voit que cette problématique s'inverse.

En parallèle de ces décisions sur l'application des correctifs, les RSSI ont travaillé au renforcement des dispositifs existants, par exemple en ajoutant des règles de détection pour les entreprises disposant d'un SIEM ou d'une surveillance par un SOC ou en mettant à jour leurs anti-malware.

Au total, sur la centaine de réponses que nous avons reçues à notre sondage sur la crise WannaCry, une entreprise – Renault – a été impactée comme vous le savez déjà. Et 4 autres adhérents du Cesin ont aussi été infectés, mais de façon plus limitée.

Est-ce la première fois que ce dilemme sur l'application des correctifs se pose aux entreprises et à leur RSSI ?

A.B. : Non. Il m'est d'ailleurs déjà arrivé d'aller voir les métiers en leur indiquant clairement qu'il fallait patcher tout de suite, faute de quoi l'activité était menacée. Mais c'est la première fois que cette question se pose à l'échelle planétaire. Clairement, nous allons devoir réétudier l'équilibre entre application des patchs et continuité des systèmes. Surtout que Microsoft se place désormais dans une logique d'évolution continue de ses systèmes. Dans une telle configuration, on ne peut plus tester chaque semaine la compatibilité de toutes les applications avec les mises à jour. Il est évident que les entreprises passent aujourd'hui trop de temps sur leurs tests de non-régression, qu'elles prennent trop de précautions en la matière.

Le constat vaut notamment pour les systèmes industriels ou métiers, particulièrement touchés par WannaCry comme l'ont montré les exemples de Renault, mais aussi du NHS (le système de santé britannique) ou de la Deutsche Bahn…

A.B. : C'est effectivement dans le monde industriel qu'on retrouve la plus forte proportion de nos membres ayant du retard dans l'application des patchs. Cette fameuse informatique industrielle connectée au SI traditionnel, mais n'évoluant pas au même rythme, pose de gros soucis. Et pas par

manque de volonté des entreprises concernées. Notons d'ailleurs que la question touche aujourd'hui aussi les RSSI ne travaillant pas dans le secteur industriel, au travers les divers capteurs, caméras connectées et autres dispositifs intégrés aux immeubles intelligents.

Pour cette informatique industrielle, les fournisseurs dévoilent de plus en plus de solutions, la plupart fondées sur le cloisonnement de ces systèmes. Est-ce une piste intéressante ?

A.B. : Ces solutions peuvent être efficaces, mais elles sont lourdes à gérer. L'idéal consisterait à sécuriser les systèmes eux-mêmes, à combler le décalage constaté aujourd'hui entre SI de gestion et SI industriel.

WannaCry est issu d'un arsenal de la NSA, tombé entre les mains d'un groupe de pirates appelé les Shadow Brokers. Récemment, c'est la CIA qui s'est fait dérober certains de ses outils de hacking, publiés par Wikileaks. N'est-ce pas une situation explosive pour les RSSI ?

A.B. : C'est effectivement un peu comme si un laboratoire médical laisser échapper des souches bactériologiques dangereuses ! Car, derrière, n'importe qui peut récupérer cette souche et la transformer en bombe. Le fait que ces agences choisissent de garder secrètes les failles zero day qu'elles ont en réserve aussi longtemps que possible sans en informer les éditeurs concernés constitue un vrai sujet.

On ne peut aujourd'hui que constater la répétition de crises systémiques. En octobre dernier, un déni de service a plongé dans le noir un pan entier d'Internet. Une forme d'attaques qui nécessite simplement de la puissance informatique. Or, il y en a aujourd'hui à revendre ! Avec WannaCry, on mesure le potentiel d'une faille zero day quand l'ensemble de la planète est assujetti aux mêmes technologies. La question de notre dépendance à une poignée de fournisseurs, concentrant des masses de données impressionnantes, se pose pleinement.

Dans un communiqué, vous adressez un satisfecit à Microsoft pour avoir sorti un correctif pour des OS qui n'étaient plus supportés, mais déplorez son « *manque de transparence* ». Pourquoi ?

A.B. : Nous aurions apprécié que Microsoft nous informe, dès avril dernier, du niveau de menace auquel nous aurions à faire face avec la faille affectant le protocole SMB. Microsoft savait alors des choses que le commun des mortels ignorait.

A lire aussi :

Thales : « les systèmes les plus critiques sont aussi les plus vulnérables à WannaCry »

WannaCry : le ransomware qui n'a plus besoin du phishing

Pour les RSSI, les solutions de cybersécurité ne sont pas satisfaisantes