Cyberattaques : comment protéger les infrastructures critiques

Dans une récente publication de l'Observatoire de l'Industrie Electrique, l'Union Française de l'Electricité (UEF) a indiqué que plus de 20 cyberattaques de grande ampleur ont concerné les systèmes énergétiques depuis 1982, avec une accélération depuis 2010.

Elle répertorie les attaques selon trois catégories : celles qui visent à exfiltrer des données confidentielles, celles cherchant à interrompre la disponibilité d'un service ou d'un système, et enfin celles ayant pour objectif d'altérer des informations ou des processus. Dans un contexte de menaces croissantes, la sécurité des infrastructures critiques, et pas seulement dans le secteur de l'énergie, est une problématique cruciale au sein des Etats.

Au quotidien, nous avons besoin d'infrastructures performantes. Qu'elles soient liées au transport, à l'énergie ou encore à l'eau, nous attendons un service sans faille. Indispensables à la vie de la nation, ce n'est pas par hasard que nous les appelons « Opérateurs d'Importance Vitale » (OIV). Cependant, aujourd'hui, nous ne vivons plus dans un monde analogique. Tout, y compris ces infrastructures, est de plus en plus connecté, ce qui entraîne une vulnérabilité accrue et une exposition plus importante à un risque physique réel. Les barrages hydrauliques, les infrastructures de communication, les chaînes de production, ou encore les réacteurs nucléaires, comprennent des éléments, des systèmes et des réseaux qui, en cas d'attaque, pourraient paralyser l'économie, la santé publique ainsi que la sécurité nationale.

Chaque pays doit prendre des mesures spécifiques pour protéger ses OIV et avoir pleinement conscience que les enjeux ne sont pas les mêmes que pour sécuriser les ressources d'un datacenter. Les infrastructures critiques sont en effet généralement réparties sur une vaste zone géographique, parfois dans des endroits déserts avec très peu de personnel sur place, ce qui rend leur sécurisation plus complexe. En outre, la majorité des éléments actifs présents dans les datacenters a une durée de vie d'environ 5 ans. La longévité d'un OIV est quant à elle extrêmement longue, et peut s'étendre de 10 à 20 ans, voire plus. Cela induit une stratégie de cybersécurité qui prenne en compte le fait que les équipements existants puissent utiliser des logiciels obsolètes ou des systèmes d'exploitation qui ne sont plus mis à jour.

De plus, de nombreux éléments relatifs aux infrastructures critiques utilisent la technologie industrielle SCADA, un système d'acquisition et de contrôle des données développé pour standardiser l'accès universel à divers modules de surveillance au sein des systèmes de contrôle industriels (ICS). Cette architecture, qui fait partie intégrante des infrastructures critiques, est particulièrement vulnérable et représente une cible de choix pour les hackers car elle permet de piloter les installations techniques à distance. Par ailleurs, et à la grande satisfaction des pirates informatiques, la plupart des communications sur ces systèmes SCADA ne sont pas chiffrées. En outre, elles nécessitent bien souvent des réponses rapides et des interactions entre les entités communicantes, faisant ainsi de ces équipements des cibles très faciles pour les attaques par déni de service (DDoS).

L'ensemble de ces caractéristiques spécifiques aux OIV, combinées à la dimension critique de certains secteurs tels que l'énergie ou encore la santé, ont fait de ces infrastructures une cible de choix pour les hackers. Alors qu'une faille de sécurité au sein d'un datacenter peut entrainer un vol

de données sensibles, une attaque similaire sur un OIV est susceptible d'avoir de graves répercussions sur la vie des citoyens, l'économie ou encore la santé. Cela a notamment été le cas par exemple en mai dernier au Royaume-Uni où de nombreux hôpitaux ont dû annuler certains actes médicaux et renvoyer des ambulances vers d'autres établissements suite à une cyberattaque.

En termes de règlementation, en France, c'est la Loi de Programmation Militaire qui impose aux OIV un certain nombre de règles de cybersécurité. Elle définit à la fois les responsabilités et les obligations pour la protection de leurs systèmes d'information critiques. Cette règlementation est appuyée par des contrôles effectués par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) ou d'autres prestataires qualifiés, chargés de s'assurer que les infrastructures critiques sont conformes aux exigences. Dans le cas contraire, une mise en demeure est adressée, puis une sanction financière en dernier recours, pouvant aller jusqu'à 150 000 euros pour les personnes physiques et 750 000 pour les personnes morales. De plus, les OIV sont tenus de notifier à l'ANSSI tout incident visant leur système de sécurité informatique (SSI).

Pour protéger les infrastructures critiques, être conformes et éviter de devoir reporter un incident aux conséquences dramatiques, il est important que les organisations effectuent des mises à jour logicielles régulières pour ne pas se retrouver avec des solutions obsolètes, et par conséquent vulnérables. De plus, une visibilité complète et continue de ce qu'il se passe sur leurs réseaux en temps réel est nécessaire à la fois sur l'équipement informatique et les technologies d'exploitation au niveau opérationnel, pour permettre une protection bien plus performante et efficace des systèmes. La détection d'une anomalie ou une activité inhabituelle dès qu'elle se produit est ainsi facilitée. Impossible en effet de sécuriser ce que l'on ne voit pas ; dès lors, les équipes en charge de la sécurité peuvent immédiatement analyser ce qu'il se passe, et prendre les mesures nécessaires, s'il s'agit d'une véritable tentative d'attaque, pour y remédier avant qu'il ne soit trop tard.

La sécurisation des Opérateurs d'Importance Vitale est particulièrement complexe et les enjeux nombreux, au même titre que les conséquences en cas de piratage. Pourtant, dans un contexte de multiplication et de sophistication des attaques, la poursuite des efforts déjà engagés en matière de cyberprotection est capitale, du point de vue des autorités, des entreprises comme des professionnels de sécurité. « La France est le premier pays à être passé par la réglementation pour mettre en place un dispositif efficace et obligatoire de cybersécurité de ces infrastructures critiques », rappelle l'ANSSI. Et c'est dans cette dynamique que la lutte contre les cybercriminels doit se poursuivre, au-delà de la règlementation.