NATIXIS
INVESTMENT MANAGERS

THEMATICS
asset management

PERSPECTIVES

Au croisement des technologies opérationnelles et des technologies de l'information : réduire les vulnérabilités en matière de cybersécurité dans les infrastructures essentielles

Frédéric Dupraz,
Gérant de portefeuille senior
Thematics Asset Management

Karen Kharmandarian,
Directeur des investissements
Thematics Asset Management

Matthieu Rolin,
Gérant de portefeuille
Thematics Asset Management

Alexandre Zilliox,
Gérant de portefeuille
Thematics Asset Management

POINTS CLES

Toutes les crises ont tendance à exposer les vulnérabilités existantes et à accélérer les mouvements de transformation. Le caractère unique de la crise du Covid-19 a jeté un nouvel éclairage sur les perturbations potentielles des infrastructures opérationnelles et technologiques, car un monde de plus en plus connecté a dû fonctionner à distance.

Dans ce monde de plus en plus connecté, il est devenu possible pour des acteurs malveillants d'infiltrer et de compromettre les systèmes des centrales nucléaires, des réseaux électriques et de régulation du trafic urbain, voire l'organisation des élections et des référendums démocratiques.

De nombreuses sociétés se sont éloignées graduellement du modèle des **technologies opérationnelles (OT)** contrôlées manuellement pour se tourner vers un environnement au sein duquel les processus physiques sont gérés au moyen d'équipements informatiques (IT) sophistiqués et interconnectés.

L'intégration IT/OT aura un impact majeur sur les structures de réseau et obligera les sociétés à concevoir des méthodes plus efficaces pour protéger le leur. L'ajout de nouveaux appareils connectés agrandit considérablement la surface d'attaque, et tout nouveau dispositif connecté peut devenir un point d'entrée pour un cyberattaquant.

Bien entendu, une fois que les failles de cybersécurité seront comblées pour les infrastructures critiques, la nature même de ce secteur implique que d'autres vulnérabilités verront le jour ailleurs dans le cyberespace. Ces spécificités font de la cybersécurité, au même titre que la sécurité des gouvernements, des individus et des sociétés plus généralement, un thème récurrent dans nos vies et dans nos investissements.

Les forces primaires qui déterminent le besoin en sécurité opérationnelle et informatique

Toutes les crises ont tendance à exposer les vulnérabilités existantes et à accélérer les mouvements de transformation. Le caractère unique de la crise du Covid-19 a jeté un nouvel éclairage sur les perturbations potentielles des infrastructures opérationnelles et technologiques, car un monde de plus en plus connecté a dû fonctionner à distance.

De nouvelles menaces et opportunités sont apparues, qui dépassent de loin tout ce que les sociétés, les gouvernements et les individus les plus éclairés auraient pu imaginer. Les causes profondes de ces perturbations ont été révélées alors que la technologie, la mondialisation, l'évolution démographique et la pénurie de ressources continuent de façonner les sociétés et les économies du monde entier. Alors que l'insécurité devient la nouvelle norme, les nations sont de plus en plus sensibles à la protection des populations et de leurs richesses à mesure que le cyber-risque s'impose comme une menace majeure.

Le sabotage à grande échelle des réseaux, systèmes et activités informatiques, communément désigné par le terme « Cybergeddon », évoque des notions de peur, de perte de contrôle et d'inévitabilité. Toutefois, si les menaces sont réelles, les opportunités le sont tout autant.

En réfléchissant à la manière dont les sociétés et les gouvernements se sont adaptés à la situation actuelle grâce aux avancées technologiques et aux progrès sociétaux, des opportunités apparaissent et peuvent conduire à une révolution industrielle axée sur le numérique. Des catalyseurs, tels que la 5G représentent une avancée décisive pour l'économie connectée, car ils libèrent le potentiel de **l'Internet des Objets (IoT)** en connectant absolument tout, des équipements d'usine aux appareils ménagers, avec une vitesse et une capacité sans précédent.

En 2019, plus de 26 milliards de dispositifs IoT étaient actifs ; d'ici 2025, on estime que 152 200 dispositifs IoT se connecteront à Internet chaque minute. Bien entendu, cette généralisation s'accompagne d'un plus grand nombre de menaces et de risques de compromission des réseaux. Pourtant, l'association de l'intelligence artificielle à la robotique pourrait également élargir le champ des possibilités dans le secteur de la production industrielle.

> Rien n'est particulièrement difficile si on le subdivise en petites tâches.
>
> **Henry Ford**, fondateur de la Ford Motor Company

Des mondes connectés

Depuis l'époque d'Henry Ford, l'industrie manufacturière a eu pour objectif de trouver des gains d'efficacité de plus en plus importants dans les processus de production. Aujourd'hui, la 5G permet à un fabricant de créer des « usines connectées », dotées de capteurs qui enregistrent des données sur absolument tout, de la température aux vibrations en passant par la quantité de matériaux utilisée. Ces avancées peuvent à leur tour générer d'énormes gains d'efficacité : la réduction des frais d'entretien grâce à la maintenance prédictive, une diminution du temps d'arrêt total des machines grâce à la surveillance et au contrôle à distance, ou même des hausses de productivité grâce au suivi en temps réel de la consommation d'énergie.

Il faut toutefois se garder de négliger la face cachée du numérique. Le pouvoir disruptif du numérique peut ouvrir des portes et donner aux cybercriminels la capacité de perturber les chaînes de valeur et de faire du vol de données et d'informations une arme extrêmement efficace. Il arrive souvent que les cyberattaques restent non détectées pendant des mois. Or, une fois les réseaux piratés, les sécuriser peut s'avérer très difficile.

Les sociétés et, de plus en plus, les gouvernements et les organismes publics sont à la merci de menaces considérables, ce qui renforce le besoin de solutions de cybersécurité de pointe. Alors que le monde s'est adapté à la migration en ligne des sociétés et des particuliers, les architectures informatiques sont en train d'être repensées de fond en comble.

À ce titre, nous ne pouvons que constater la nécessité pour les agents économiques de remédier aux vulnérabilités en matière de cybersécurité afin de sauvegarder les infrastructures essentielles et d'assurer le bon fonctionnement des marchés et des économies.

Technologie opérationnelle (OT)

Matériel et logiciels qui détectent ou provoquent un changement, par la surveillance et/ou le contrôle direct des équipements, des actifs, des processus et des évènements industriels.

Internet des Objets (IoT)

Le terme Internet des Objets désigne le réseau d'objets physiques qui intègrent des capteurs, des logiciels et d'autres technologies et qui se connectent ou échangent des données avec d'autres appareils et systèmes via Internet.

La frontière mouvante de la cybersécurité

Dans ce monde de plus en plus connecté, il est devenu possible pour des acteurs malveillants d'infiltrer et de compromettre les systèmes des centrales nucléaires, des réseaux électriques et de régulation du trafic urbain, voire l'organisation des élections et des référendums démocratiques. Plus la quantité de connexions augmente, plus les possibilités de piratage se multiplient.

L'ampleur du défi auquel doit faire face le secteur de la cybersécurité est considérable. Il suffit de se souvenir de l'incident de 2013. Au cours d'un après-midi d'avril, la totalité d'Internet, à savoir les 3,7 milliards d'ordinateurs et d'appareils connectés dans les usines, les poches et les bureaux du monde entier, ont reçu un ping de la part d'un seul opérateur.

Ce ping a révélé que près de 114 000 systèmes de contrôle de fabrication étaient vulnérables à une attaque, dont environ 13 000 pouvaient être accessibles sans avoir à saisir un seul mot de passe. À lui seul, cet évènement a servi de signal d'alarme pour le secteur de la cybersécurité.

Bombes logiques et vers informatiques

L'un des exemples les plus anciens d'un piratage industriel dévastateur date de 1982. La CIA réussit à injecter une « bombe logique » dans le système **SCADA (Système de contrôle et d'acquisition des données)** de contrôle des gazoducs sibériens de l'URSS. Le résultat a été ce que le Washington Post a appelé « l'explosion et l'incendie non-nucléaires les plus monumentaux jamais observés depuis l'espace[1] ».

Un système SCADA est une application informatique destinée à surveiller et contrôler une usine ou un équipement au niveau de la supervision. Ce type de système est utilisé dans de nombreux secteurs d'activité pour collecter et analyser des données en temps réel, ainsi que pour contrôler des fonctions. Cela en fait une cible de choix pour les pirates informatiques. C'est pourquoi il est important de défendre votre système contre les menaces et les attaques visant les environnements SCADA.

En 2010, l'attaque Stuxnet a lancé un signal d'alarme pour les systèmes SCADA du monde entier. Comptant parmi l'un des **malwares** les plus complexes à ce jour, il est considéré comme la première menace connue ciblant spécifiquement les systèmes SCADA en vue de contrôler les réseaux.

Apparemment conçue sous l'égide de gouvernements étrangers, l'attaque du ver informatique Stuxnet a ciblé les **Automates Programmables Industriels (API ou PLC pour Programmable Logic Controller)** des installations nucléaires iraniennes, accélérant la vitesse de rotation des centrifugeuses sans déclencher d'alarme. Avant d'être détectée, l'attaque a permis de détruire quasiment un cinquième des centrifugeuses nucléaires du pays et de faire reculer son programme nucléaire d'une décennie.

L'une des leçons tirées de l'attaque Stuxnet est qu'une menace sophistiquée peut réellement cibler n'importe quel système, si bien que la capacité de détection et de restauration après une cyberattaque est fondamentale. En mai 2012, le laboratoire russe Kaspersky, l'un des plus grands éditeurs mondiaux de logiciels antivirus, a découvert un autre virus hautement sophistiqué visant l'Iran.

Contrairement à Stuxnet, le virus Flame, qui est resté non détecté pendant des années, était conçu pour dérober des fichiers PDF et des plans **AutoCAD**. Cela signifie que l'auteur de l'attaque ciblait les concepts, les plans et les données IP précieusement gardées, conservées sous clé dans certaines des plus grandes installations industrielles du pays[2].

Des barrages aux réseaux électriques

En 2013, des pirates informatiques iraniens sont parvenus à accéder au système de contrôle d'un barrage de l'État de New York. Cette intrusion était loin d'être élaborée, puisqu'elle constituait simplement un test de la part des attaquants pour identifier les possibilités d'accès. Bowman Dam est un petit fournisseur d'électricité qui permet de réguler les crues liées aux tempêtes. Son système SCADA était connecté à Internet via un modem cellulaire. Avec un système SCADA en maintenance au moment de l'attaque, aucune fonction de contrôle n'était disponible, excepté la surveillance de l'état.

Il semblerait que le barrage ait été attaqué en raison de la vulnérabilité de sa connexion Internet et de l'absence de contrôles de sécurité, plutôt que dans le cadre d'une cyberattaque ciblée. Bien que l'on ignore l'identité de ceux qui ont mené l'intrusion, on connaît la sophistication technique dont les pirates ont fait preuve en manipulant directement l'équipement SCADA. Cet incident rappelle une fois de plus que lorsque les systèmes SCADA sont directement exposés à Internet, ils deviennent une cible facile pour tout cybercriminel potentiel[3].

Deux ans après le piratage du barrage Bowman, la première cyberattaque réussie connue contre un réseau électrique

Automates Programmables Industriels (PLC)

Ordinateurs industriels robustes et adaptés au contrôle des processus de production, tels que les chaînes de montage, les équipements robotiques ou toute activité nécessitant une grande fiabilité, une facilité de programmation et un diagnostic des défaillances du processus.

Dessin AutoCAD

Illustration détaillée en 2D ou 3D montrant les composants d'un projet d'ingénierie ou d'architecture.

Système de contrôle et d'acquisition des données (SCADA)

Architecture de système de contrôle incluant des ordinateurs, des communications de données en réseau et des interfaces graphiques utilisateurs (GUI) pour la gestion de supervision des processus de haut niveau, et qui inclut également d'autres dispositifs périphériques tels que des contrôleurs logiques programmables (PLC) et des contrôleurs Proportionnel-Intégral-Dérivé (PID) discrets pour l'interface avec l'usine ou des machines.

Logiciel malveillant (malware)

Terme générique utilisé pour désigner plusieurs types de logiciels intrusifs ou hostiles : virus ou ver informatique, cheval de Troie, rançongiciel, logiciel espion, ad-ware, scareware, etc.

d'électricité près d'un quart de millions d'Ukrainiens. Les attaquants ont coupé le courant pour 30 postes électriques, privant d'électricité environ 230 000 personnes pendant 6 heures.

Ils se sont servis **d'e-mails de harponnage (spear phishing)**, une approche peu sophistiquée pour ce type d'attaques, mais qui reste d'actualité, puisque des attaques de hameçonnage sont encore menées contre des infrastructures essentielles. La sensibilisation à ce type de risques est donc un facteur décisif dans le succès ou l'échec de ces approches simplistes.

Un an exactement après cette attaque, une autre attaque a frappé le pays, visant cette fois le poste électrique de Pivichna, près de Kiev, et provoquant une panne d'électricité d'une heure dans les environs. Cette attaque revêt une importance particulière, car elle a conduit à se demander si toutes ces attaques n'annonçaient pas une offensive encore plus puissante.

En effet, Eugene Kaspersky, expert en cybersécurité et PDG de Kaspersky Labs, a lancé un avertissement au monde entier, indiquant que nous pourrions être à l'aube d'une crise majeure, puisque les pirates semblent cibler les fonctionnalités des infrastructures essentielles[4].

Pirater les pacemakers et exposer les prisons

Le piratage des infrastructures peut même s'étendre aux implants médicaux, qui sont considérés par certains comme la « nouvelle frontière ». En 2019, des régulateurs et des experts en sécurité américains ont publié un avertissement officiel indiquant que les pirates pouvaient désormais accéder aux équipements médicaux essentiels, dont les pacemakers et les pompes à insuline, avec des résultats potentiellement dévastateurs[5].

Puis, début 2020, des pirates ont secrètement pénétré dans les systèmes d'une société informatique américaine, SolarWinds, qui comptait 33 000 clients, dont des sociétés du Fortune 500 telles que Microsoft, Cisco, Intel et Deloitte, ainsi que des agences gouvernementales américaines, parmi lesquelles le Département du Trésor. La cyberattaque est passée inaperçue pendant des mois et de nombreux réseaux ont été compromis sans qu'il soit possible de remédier rapidement au problème.

Le gouvernement américain a en effet confirmé que la sécurisation des réseaux pourrait prendre des années. En raison du fait qu'elle a exposé non seulement les grandes entreprises mais aussi les agences gouvernementales à des attaques, elle demeure la plus grande faille de sécurité de ces dernières années.

Un autre exemple récent est celui d'un groupe de hackers qui est parvenu à pirater les données de caméras de sécurité collectées par des sociétés de la Silicon Valley, ce qui leur a permis d'accéder aux flux vidéo en temps réel de 150 000 caméras de surveillance dans des hôpitaux, des entreprises, des services de police, des prisons et des écoles. Le constructeur automobile Tesla figure parmi les sociétés dont les images ont été divulguées.

Certaines de ces caméras utilisaient une technologie de reconnaissance faciale pour identifier et catégoriser les personnes filmées. L'une des vidéos montre même des agents dans un poste de police de Stoughton (Wisconsin), en train d'interroger un homme menotté. Avez-vous déjà imaginé que votre identité puisse être exposée ainsi ? Si oui, achèteriez-vous encore des caméras de sécurité auprès de cette société ?

En outre, l'inflation réglementaire mondiale amène les gouvernements, les entreprises et les particuliers à prendre davantage conscience des enjeux liés à la sécurité en matière de confidentialité et de protection des données. Cette prise de conscience mène à des investissements importants dans les solutions de cybersécurité.

Quand la sécurité informatique rencontre la sécurité opérationnelle

Alors, pourquoi toutes ces attaques ? Et comment la situation va-t-elle évoluer à l'avenir ?

En résumé, à mesure que la technologie continue d'évoluer, de nombreuses organisations s'éloignent graduellement des systèmes de technologie opérationnelle (OT) isolés et contrôlés manuellement pour se tourner vers un environnement au sein duquel les processus physiques sont contrôlés au moyen d'équipements informatiques (IT) sophistiqués et interconnectés.

Comme un nombre croissant d'appareils deviennent « intelligents » grâce à la connectivité sans fil, les systèmes OT qui demandaient autrefois une manipulation manuelle, comme le réglage d'une vanne ou l'actionnement d'un interrupteur, peuvent désormais être contrôlés à distance. Nombre de ces systèmes OT font désormais partie de l'infrastructure essentielle d'une organisation.

Prenez la NASA. Ses systèmes OT sont utilisés pour tester les systèmes de propulsion des

E-mails de harponnage (spear phishing)

Le harponnage est un type d'attaque par e-mail ou par communication électronique visant une personne, une organisation ou une société en particulier.

fusées, contrôler et communiquer avec les engins spatiaux, et faire fonctionner les installations au sol. Ils interviennent également dans la gestion de l'énergie électrique, des systèmes de chauffage et de climatisation ainsi que d'autres infrastructures connexes.

Si la convergence des technologies de l'information et des technologies opérationnelles peut permettre de réaliser des économies et d'autres gains d'efficacité, elle signifie également que les systèmes OT sont potentiellement vulnérables aux problèmes de sécurité qui affectent habituellement les systèmes informatiques, notamment le piratage[6].

Le défi cyberphysique et la nécessité pour les infrastructures vieillissantes de s'adapter à une surface de plus en plus connectée

L'intégration des OT avec les IT aura un impact énorme sur les structures de réseau et obligera les sociétés à concevoir des méthodes plus efficaces pour protéger le leur. L'ajout de nouveaux appareils connectés agrandit considérablement la surface d'attaque, et tout nouveau dispositif connecté peut devenir un point d'entrée pour un cyberattaquant. L'ancienne architecture « castle and moat » ("château et douves") est aujourd'hui obsolète et prête à disparaître.

L'approche « castle and moat »

Imaginons un château entouré de douves profondes. Le seul moyen pour entrer et sortir du château est un pont-levis fortement gardé. Toute personne qui tente de pénétrer dans le château doit passer un contrôle de sécurité strict effectué par les gardes. Une fois que l'identité de cette personne est validée, elle peut accéder librement au château et à tout ce qu'il contient. En fait, à l'intérieur du château, tout le monde est digne de confiance par défaut.

C'est là que réside le problème : si quelqu'un parvient à contourner les gardes et à entrer dans le château sans autorisation, il ne sera plus jamais contrôlé, et il sera libre d'aller et venir dans le château sans contrainte. Imaginez maintenant que l'on multiplie le nombre de portes d'entrée : cela multipliera le risque que des intrus se promènent dans le château en toute impunité.

C'est pourquoi la sécurité des réseaux a besoin d'un nouveau modèle : l'approche « confiance zéro » (zero-trust).

L'approche « confiance zéro »

L'approche **« confiance zéro »** est radicalement différente du modèle « castle and moat ». La sécurité de confiance zéro implique que personne ne soit digne de confiance par défaut, que ce soit à l'intérieur ou à l'extérieur d'un réseau d'entreprise, si bien qu'une vérification est requise pour quiconque souhaite accéder aux ressources du réseau.

Ce modèle exige une vérification stricte de l'identité de toute personne et de tout appareil tentant d'accéder aux ressources d'un réseau privé, qu'ils soient dans ou hors du périmètre du réseau d'entreprise. L'identité devient l'élément central, ce qui signifie que l'on peut multiplier les points d'entrée sur le réseau sans aucun problème, puisqu'il est à chaque fois nécessaire de prouver son identité.

Les catalyseurs perturbateurs qui forcent la convergence des TO et des TI

L'impact de l'IA et de l'automatisation sur l'industrie

Lorsque l'on parle d'Intelligence artificielle (IA) et d'automatisation en cybersécurité, dans la plupart des cas, il est question de **l'Apprentissage automatique (ou Machine Learning)**. L'apprentissage automatique est un sous-ensemble de l'IA dont l'objectif est d'apprendre à une machine à prendre une décision par elle-même ou à répondre à une question sans qu'il soit nécessaire de lui donner des instructions très précises ou de la programmer afin d'inclure toutes les possibilités.

Comment l'IA et l'apprentissage automatique transforment-ils l'industrie ?

En termes simples, les humains et les solutions traditionnelles de cybersécurité ne sont plus suffisants aujourd'hui :

- Les solutions traditionnelles surveillent, analysent et examinent les menaces et les risques connus, tandis que les solutions basées sur l'apprentissage automatique peuvent permettre de détecter de nouvelles anomalies (malwares, virus, etc.), de prévenir l'attaque et d'orchestrer une réponse, le cas échéant. Si nous prenons l'exemple de **l'authentification multifacteur (MFA)**, les outils d'apprentissage automatique pourraient détecter tout utilisateur qui se connecterait au réseau à partir d'un appareil ou d'un emplacement inconnu, et réagir en bloquant l'accès ou en exigeant un autre facteur d'authentification (mot de passe unique, reconnaissance

Confiance zéro (Zero Trust)

Une approche de conception et de mise en œuvre des infrastructures informatiques. Le concept de la confiance zéro est que les appareils ne doivent pas être validés par défaut, même s'ils sont connectés au réseau géré de la société et qu'ils ont été vérifiés précédemment.

Apprentissage automatique (Machine Learning)

L'étude d'algorithmes informatiques qui s'améliorent automatiquement par le biais de l'expérience et par l'exploitation des données.

Authentification multifacteur (MFA)

Une méthode d'authentification électronique au moyen de laquelle un utilisateur n'est autorisé à accéder à un site web ou à une application qu'après avoir présenté avec succès deux ou plusieurs éléments de preuve à un mécanisme d'authentification.

faciale, numérisation d'empreintes digitales, etc.). Les solutions traditionnelles ne tiennent généralement pas compte de l'historique du comportement d'un utilisateur, d'un appareil ou d'un réseau, ce qui augmente les possibilités de réussite d'une attaque.

- Le nombre de dispositifs qui doivent être protégés est désormais gigantesque : qu'il s'agisse d'ordinateurs, de smartphones, de serveurs, de machines industrielles ou de voitures, tout est connecté, ce qui augmente la surface d'attaque. Les humains ne peuvent tout simplement pas analyser toutes les menaces et les comportements anormaux qui se produisent dans les sociétés. C'est là qu'interviennent l'automatisation et l'IA. Ainsi, CrowdStrike, l'un des principaux fournisseurs de solutions de sécurité des points de terminaison qui compte près de 10 000 clients, capture plus de 5 trillions d'évènements par semaine sur sa plateforme.

5G : une plus grande connectivité et des systèmes interfacés entraînent une plus grande vulnérabilité des infrastructures essentielles

Par rapport à la 4G, la norme 5G offre deux caractéristiques essentielles :

1. la possibilité de connecter plus de mille fois plus d'objets au réseau,
2. une latence réduite à 1 milliseconde.

Ce sont ces deux caractéristiques qui seront utilisées pour connecter l'appareil productif. En effet, une faible latence est un élément essentiel pour prendre le contrôle d'une machine ou d'un robot, puisque les commandes données doivent être reçues instantanément par l'équipement connecté. Parallèlement, la capacité de connecter un très grand nombre d'objets est également essentielle pour pouvoir contrôler une grande flotte d'appareils.

Les sociétés seront également en mesure de créer des réseaux 5G privés, plus rapides et mieux adaptés que les réseaux Wifi, afin de connecter les technologies opérationnelles. Les principales interrogations qui subsistent concernent le taux d'adoption de la 5G et la mise en œuvre de cette technologie.

Les implications de la relocalisation

La pandémie de Covid-19 a révélé que la dépendance excessive à l'égard de régions du monde éloignées pour la fabrication pose des risques tant économiques qu'au niveau de la sécurité nationale. Les gouvernements du monde entier en ont pris bonne note et l'on voit se multiplier les incitations à la relocalisation de certaines de ces capacités de production à proximité de la demande. Le dernier exemple en date, et peut-être le plus frappant, concerne le secteur des semi-conducteurs, qui est probablement confrontée au plus grand épisode de pénurie de son histoire. Cette situation affecte plusieurs marchés finaux, notamment l'électronique grand public, l'automobile et l'industrie.

Cette tendance à la relocalisation s'observe principalement dans les économies développées qui, dans la plupart des cas, ont sous-investi dans leurs installations industrielles et/ou délocalisé leurs sites de fabrication dans des pays où la main-d'œuvre est à faible coût depuis des décennies. On peut dès lors s'attendre à ce que les sociétés et les gouvernements tentent de mettre en place des capacités de production modernes, ce qui devrait entraîner une hausse de la demande de machines, d'appareils et de plateformes logicielles connectés qui traiteront les données générées au niveau de la fabrication.

En somme, cette modernisation pourrait agir comme un catalyseur pour la mise en place de **l'industrie 4.0 et de l'Internet Industriel des Objets (IIdO)**: McKinsey estime que le marché de l'IIdO devrait connaître une croissance annuelle de 12 % jusqu'à 2025, et pourrait atteindre un volume de marché de 500 milliards de dollars[7], le tout soutenu par le déploiement de la 5G. Ce développement entraînera également la nécessité de sécuriser les outils susmentionnés, ainsi que les données qui en découlent, ce qui crée un nouveau domaine de croissance pour la cybersécurité.

Les catalyseurs perturbateurs qui forcent la convergence des TO et des TI

Il y a une dizaine d'années, les discussions sur la protection des sociétés contre les pirates informatiques tournaient essentiellement autours de la protection des serveurs ou des équipements informatiques au sens large, à savoir la protection de l'équipement physique. C'est le passage du stockage physique au stockage virtuel, c'est-à-dire l'informatique en nuage (ou Cloud Computing), et la connectivité croissante des technologies opérationnelles qui ont complètement changé la façon dont les sociétés doivent envisager la cybersécurité.

Qui plus est, l'une des conséquences de la pandémie a été l'attention accrue portée à la sécurité des télétravailleurs. De nombreux employés utilisent leurs appareils personnels pour l'authentification à deux facteurs, et se servent également des versions mobiles des applications telles que Teams et Zoom pour la messagerie instantanée et les visioconférences avec les clients. Les frontières entre la vie personnelle et la vie professionnelle s'estompent, ce qui ne fait qu'augmenter le risque que des informations sensibles finissent dans un environnement non sécurisé.

Internet industriel des objets (IIdO)

Désigne des capteurs, des instruments et d'autres dispositifs interconnectés et mis en réseau avec les applications industrielles des ordinateurs, notamment dans le secteur de la fabrication et celui de la gestion de l'énergie.

Selon une étude du géant de la technologie réseau Cisco, 52 % des personnes interrogées ont déclaré que les appareils mobiles constituaient un défi majeur en matière de cybersécurité[8]. Il est évident que les sociétés ne sont pas uniquement tenues de protéger leurs systèmes et leur lieu de travail au sens physique, elles doivent aussi assurer leur protection au sens virtuel, tout en veillant à ce que les connexions à distance aux systèmes et lieux de travail virtuels, que ce soit via un appareil fourni par la société ou un appareil personnel, soient à la fois autorisées et sécurisées.

Il n'est donc pas étonnant que, d'après les prévisions, les dépenses mondiales en technologies et en services de sécurité informatique et de gestion des risques prévoient d'augmenter de 12,4 % pour atteindre 150,4 milliards de dollars en 2021 : en effet, 61 % des 2 000 responsables informatiques interrogés s'attendaient à une augmentation des dépenses en cybersécurité en 2021[9].

Les solutions et les services actuellement disponibles pour lutter contre les cybercriminels et protéger les activités numériques se répartissent en quatre grandes catégories :

1. La sécurité des centres de données – Selon le dernier rapport IDC-MarketScape sur[10] le marché des services de collocation et d'interconnexion, le segment des centres de données a présenté des performances supérieures à la moyenne des technologies informatiques au cours des 18 derniers mois, soutenu par la demande de plateformes numériques que la pandémie de Covid-19 a engendré. Le rapport cite Equinix et Digital Reality Trust comme étant deux fournisseurs qui proposent des portefeuilles multicouches répondant aux exigences actuelles et émergentes de la plupart des sociétés en matière d'infrastructure numérique.
2. Les logiciels et services de cybersécurité : l'un des leaders dans ce domaine est la société Zscaler, basée en Californie. Son modèle de sécurité en cloud est conçu pour applications cloud et de mobilité, ce qui lui permet d'être déployé partout où une organisation dispose de ressources, y compris dans les bureaux à domicile. La société propose un échange de confiance zéro, où son Cloud agit comme un hub centralisé qui permet aux ressources de se connecter les unes aux autres : les applications protégées derrière l'échange de confiance zéro ne sont pas visibles et ne peuvent pas être découvertes, ce qui élimine la surface d'attaque. Un autre leader du marché est Varonis, dont le siège social est à New York, et qui fournit une plateforme logicielle de sécurité pour permettre aux organisations de suivre, de visualiser, d'analyser et de protéger leurs données non structurées. La société analyse le comportement des utilisateurs pour identifier les comportements anormaux et protéger les données des sociétés contre les cyberattaques. Son logiciel extrait les métadonnées de l'infrastructure informatique d'une société et utilise ces informations pour cartographier les relations entre les employés, les objets de données, les contenus et les utilisations, ce qui permet aux organisations d'avoir une meilleure visibilité sur leurs données et de protéger leurs informations essentielles et sensibles.
3. Les puces de cybersécurité : depuis de nombreuses années, la société californienne Nvidia fournit les GPU (processeurs graphiques) utilisés dans les centres de données et les superordinateurs pour réaliser les simulations 3D. Toutefois, en 2021, elle a annoncé qu'elle se positionnait sur le marché des CPU (unités centrales de traitement) pour serveurs avec une nouvelle puce construite sur l'architecture ARM. Ce processeur, dont le nom de code est Grace, ne sera pas commercialisé avant le début 2023. Nvidia affirme que la puce offrira des performances 10 fois supérieures à celles des principales puces de serveurs x86 pour les applications d'IA et le traitement des gros volumes de travail en data science. Selon certains, ce produit pourrait constituer une menace concurrentielle pour Intel, qui domine depuis longtemps le marché des puces serveurs[11].
4. La cyberassurance : le marché mondial de la cyberassurance devrait atteindre 24 185,3 millions de dollars d'ici à 2025, selon les estimations de Market Research Future (MRFR) dans son rapport de 2020[12]. La demande de services de cyberassurance devrait augmenter rapidement pendant la période de prévision (2020-2027) en raison de l'adoption de la blockchain et des logiciels d'analyse des risques. Les analyses de risques sont utilisées par les souscripteurs pour analyser l'évaluation des primes sur les actifs et les solutions numériques. L'accélération de la vitesse des transactions et des règlements sans intermédiaire peut faciliter la demande. En outre, la demande d'une couverture des risques propres par les assureurs en raison d'une plus grande présence en ligne peut stimuler le marché mondial de la cyberassurance. Beazley, le spécialiste londonien de l'assurance, est l'un des leaders du marché.

D'après les prévisions, les dépenses mondiales en technologies et en services de sécurité informatique et de gestion des risques devraient augmenter de **12,4 %** pour atteindre **150,4 milliards de dollars** en 2021 : en effet, **61 %** des **2 000 responsables informatiques** interrogés s'attendaient à une augmentation des dépenses en cybersécurité en 2021[9].

Une opportunité à saisir

Il est difficile d'estimer l'ampleur de cette opportunité, car elle est encore naissante, et très peu de sociétés communiquent sur les TO ou disposent de solutions dédiées aux TO.

En effet, la connexion d'un appareil opérationnel à un réseau est identique à la connexion de n'importe quel appareil. L'architecture de confiance zéro ne se soucie pas du type d'appareil qui se connecte au réseau. Ce qui compte est l'identité de cet appareil.

Les solutions de sécurité des points de terminaison se concentreront sur les TO, tandis que l'informatique de périphérie (ou Edge Computing) est encore balbutiante et requiert des solutions de sécurité spécifiques. L'informatique de périphérie est un paradigme d'informatique distribuée qui rapproche les calculs et le stockage des données de l'endroit où ils sont nécessaires afin d'améliorer les temps de réponse et d'économiser la bande passante.

Elle est à l'opposé du modèle centralisé de type « Full Cloud » et va se développer parallèlement au développement de l'IdO et des TO connectées. Cela dit, Crowdstrike, le leader mondial des solutions de point de terminaison, estime que son marché adressable total atteindra 106 milliards de dollars d'ici à fin 2025, contre 36 milliards de dollars en 2021.

Investir aujourd'hui dans le monde de demain

S'il est clair que nous entrons dans une nouvelle phase de l'évolution de la cybersécurité qui ressemblera peu à ce qu'elle était il y a 10 ans à peine, du point de vue de l'investissement, nous devons nous rappeler que les vecteurs de cette évolution restent les mêmes. De manière générale, il s'agit de la numérisation, de l'innovation, de la réglementation et de la mondialisation.

La différence réside dans le rythme auquel ces vecteurs peuvent accélérer et perturber la croissance des marchés et des sociétés. Il existera toujours des sociétés qui manqueront la prochaine opportunité et passeront du statut d'innovateur à celui de fournisseur traditionnel. C'est le fameux « piège technologique » dans lequel sont tombées de nombreuses sociétés, dont la plus tristement célèbre est peut-être Kodak.

En outre, le passage d'une sécurité informatique basée sur le périmètre à une sécurité dans le Cloud a donné naissance à des défis et des technologies associées totalement différents.

Il est donc essentiel de se tenir informé des dernières innovations et de s'intéresser de près à la prochaine orientation que pourrait prendre la cybersécurité.

La pandémie a eu un impact supplémentaire et a modifié les modes de travail, ce qui a encore accéléré le rythme du changement. Les sociétés et les gouvernements ont donc un rôle majeur à jouer pour remédier aux vulnérabilités des infrastructures essentielles en matière de cybersécurité, et le temps presse. Il ne s'agira pas seulement de se protéger contre un piratage ou une infraction, mais également d'élaborer des plans et des politiques plus stricts et mieux coordonnés pour définir les mesures à prendre en cas d'infraction ou de piratage.

En 2021, nous avons assisté aux attaques de cybersécurité de l'oléoduc de Colonial Pipeline, le plus grand oléoduc des États-Unis, ainsi que du géant de l'agroalimentaire mondial, JBS Foods. Dans les deux cas, les sociétés ont payé les rançons réclamées par les cybercriminels, soit 4 millions de dollars pour Colonial Pipeline[13] et 11 millions de dollars pour JBS Foods[14].

Le paiement d'une rançon est la solution la moins souhaitable. Comme l'explique Jeff Lanza, expert en cybersécurité et ancien agent du FBI : « *Ne payez pas la rançon pour trois raisons. Tout d'abord, vous n'avez aucune garantie que vous allez récupérer vos informations et la clé de chiffrement. En général, c'est le cas, mais il n'y a aucune garantie. Deuxièmement, si vous payez, vous êtes étiqueté comme payeur et vous risquez une nouvelle attaque. Troisièmement, lorsque quelqu'un paie une rançon, cet argent peut être utilisé pour financer d'autres activités criminelles (comme la traite des êtres humains et le terrorisme) et les criminels obtiennent généralement l'argent nécessaire pour financer de grandes opérations en menant des attaques par rançongiciel. En payant la rançon, vous êtes susceptible d'encourager d'autres activités illégales.* »

Bien entendu, une fois qu'il aura été remédié aux lacunes en matière de cybersécurité des infrastructures essentielles, la nature même de ce secteur implique que d'autres vulnérabilités verront le jour ailleurs dans le cyberespace. Ces spécificités font de la cybersécurité, au même titre que la sécurité des gouvernements, des individus et des sociétés plus généralement, un thème récurrent dans nos vies et dans nos investissements.

> Ne payez pas la rançon pour trois raisons. Tout d'abord, vous n'avez aucune garantie que vous allez récupérer vos informations et la clé de chiffrement. En général, c'est le cas, mais il n'y a aucune garantie. Deuxièmement, si vous payez, vous êtes étiqueté comme payeur et vous risquez une nouvelle attaque. Troisièmement, lorsque quelqu'un paie une rançon, cet argent peut être utilisé pour financer d'autres activités criminelles (comme la traite des êtres humains et le terrorisme) et les criminels obtiennent généralement l'argent nécessaire pour financer de grandes opérations en menant des attaques par rançongiciel. En payant la rançon, vous êtes susceptible d'encourager d'autres activités illégales.
>
> **Jeff Lanza**, expert en cybersécurité et ancien agent du FBI

RÉFÉRENCES

1. Source : https://www.industryweek.com/technology-and-iiot/media-gallery/21962962/11-biggest-industrial-cyberattacks-so-far-slideshow/slideshow?slide=1
2. Source : https://www.dpstele.com/blog/major-scada-hacks.php
3. Source : https://www.dpstele.com/blog/major-scada-hacks.php
4. Source : https://www.cbronline.com/cybersecurity/top-5-infrastructure-hacks/
5. Source : https://www.industryweek.com/technology-and-iiot/article/21960609/manufacturers-of-medical-devices-warned-about-hacking
6. Source : https://oig.nasa.gov/audits/reports/FY17/IG-17-011.pdf
7. Source : https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/a%20manufacturers%20guide%20to%20generating%20value%20at%20scale%20with%20iiot/leveraging-industrial-iot-and-advanced-technologies-for-digital-transformation.pdf
8. Source : https://www.cisco.com/c/en_uk/products/security/ciso-benchmark-report-2020.html
9. Source : https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-management
10. Source : https://www.equinix.se/resources/analyst-reports/interconnection-colocation-equinix-idc-marketscape
11. Source : https://www.pcmag.com/news/nvidia-unveils-a-cpu-chip-for-data-centers-supercomputers
12. Source : https://www.globenewswire.com/news-release/2021/06/14/2246715/0/en/Cyber-Insurance-Market-Valuation-to-Reach-USD-24-185-3-Million-by-2025-with-28-61-CAGR-IT-and-Telecom-Sector-is-Expected-to-Register-33-24-CAGR-by-2025.html
13. Source : https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password?sref=ialMV164
14. Source : https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781

NATIXIS
INVESTMENT MANAGERS

Mentions Légales

Le présent document est fourni uniquement à des fins d'information aux prestataires de services d'investissement ou aux autres Clients Professionnels ou Investisseurs Qualifiés et, lorsque la réglementation locale l'exige, uniquement sur demande écrite de leur part. Le présent document ne peut pas être utilisé auprès des clients non-professionnels. Il relève de la responsabilité de chaque prestataire de services d'investissement de s'assurer que l'offre ou la vente de titres de fonds d'investissement ou de services d'investissement de tiers à ses clients respecte la législation nationale applicable.

En France: Le présent document est fourni par Natixis Investment Managers International - Société de gestion de portefeuilles agréée par l'Autorité des Marchés Financiers sous le n° GP 90-009, société anonyme immatriculée au RCS de Paris sous le numéro 329 450 738. Siège social: 43 avenue Pierre Mendès France, 75013 Paris.
Au Luxembourg: Le présent document est fourni par Natixis Investment Managers S.A. – Société de gestion luxembourgeoise agréée par la Commission de Surveillance du Secteur Financier, société anonyme immatriculée au RCS de Luxembourg sous le numéro B115843. 2, rue Jean Monnet, L-2180 Luxembourg, Grand-Duché de Luxembourg.
En Belgique: Le présent document est fourni par Natixis Investment Managers S.A., Belgian Branch, Gare Maritime, Rue Picard 7, Bte 100, 1000 Bruxelles, Belgique
En Suisse Le présent document est fourni par Natixis Investment Managers, Switzerland Sàrl, Rue du Vieux Collège 10, 1204 Genève, Suisse ou son bureau de représentation à Zurich, Schweizergasse 6, 8001 Zürich.
Les entités susmentionnées sont des unités de développement commercial de Natixis Investment Managers, la holding d'un ensemble divers d'entités de gestion et de distribution de placements spécialisés présentes dans le monde entier. Les filiales de gestion et de distribution de Natixis Investment Managers mènent des activités réglementées uniquement dans et à partir des pays où elles sont autorisées. Les services qu'elles proposent et les produits qu'elles gèrent ne s'adressent pas à tous les investisseurs dans tous les pays.

Bien que Natixis Investment Managers considère les informations fournies dans le présent document comme fiables, y compris celles des tierces parties, elle ne garantit pas l'exactitude, l'adéquation ou le caractère complet de ces informations.

La remise du présent document et/ou une référence à des valeurs mobilières, des secteurs ou des marchés spécifiques dans le présent document ne constitue en aucun cas un conseil en investissement, une recommandation ou une sollicitation d'achat ou de vente de valeurs mobilières, ou une offre de services. Les investisseurs doivent examiner attentivement les objectifs d'investissements, les risques et les frais relatifs à tout investissement avant d'investir. Les analyses et les opinions mentionnées dans le présent document représentent le point de vue de (des) l'auteur (s) référencé(s). Elles sont émises à la date indiquée, sont susceptibles de changer et ne sauraient être interprétées comme possédant une quelconque valeur contractuelle.

Le présent document ne peut pas être distribué, publié ou reproduit, en totalité ou en partie.

Tous les montants indiqués sont exprimés en USD, sauf indication contraire.

THEMATICS ASSET MANAGEMENT
Un affilié de Natixis Investment Managers.
Société par actions simplifiée au capital social de 191 440 €.
RCS Paris 843 939 992
Agréée par l'Autorité des Marchés Financiers (AMF), sous le numéro GP 19000027.
20 rue des Capucines, 75002 Paris
www.thematics-am.com

NATIXIS INVESTMENT MANAGERS
RCS Paris 329 450 738. Capital social : 178 251 690 €
43 avenue Pierre Mendès France, 75013 Paris
www.im.natixis.com

INT533-0621