dossier.

Kleine Geräte, grosses Risiko

IoT-Cybersecurity | Das Internet der Dinge bringt spannende Entwicklungen – und Nachholbedarf bei der Cybersecurity. Auch weil es nun technisch möglich ist, über Grenzen hinweg zu handeln, ohne sie physisch überschreiten zu müssen.

Petits dispositifs, gros risques

Cybersécurité de l'IoT | L'Internet des objets est synonyme de développements passionnants – et de retard en matière de cybersécurité. Et ce, aussi parce qu'il est désormais techniquement possible d'agir au-delà des frontières sans avoir à les franchir physiquement.

Bild | Figure: Wyss Institute at Harvard University

MONIKA FREUNEK

Kaum bemerkt von der Öffentlichkeit hat sich die geopolitische Lage der Cybersecurity beim Internet of Things, IoT, in den letzten Monaten gravierend verschärft. Lange galt die stillschweigende Annahme, dass international vor offenen Cyberangriffen auf Infrastrukturen durch staatliche Akteure und als Mittel zur Verfolgung strategischer und militärischer Ziele weitestgehend zurückgeschreckt wird.

Diese Annahme wird mit einem Blick auf den Hintergrund insbesondere des Zusammenspiels von internationalem Kriegsrecht, militärischer Strategie und Cybersecurity besser verständlich. Das Aufkommen von Computern und deren integrale Vernetzung in die Gesellschaft haben es technisch möglich gemacht, über Grenzen hinweg zu handeln, ohne sie physisch überschreiten zu müssen. Technische Mittel ermöglichen es auch, geografische Spuren von Computeraktivitäten zu verschleiern oder gar falsche Spuren zu legen. Damit ist die sichere Zuordnung von Akteuren schwierig bis unmöglich. Dies ist in der klassischen Kriegsführung, dem kinetischen Krieg, anders: Ein Panzer, der eine Landesgrenze überschreitet, ist klar als solcher erkennbar, und ebenso ist die Überschreitung einer Grenze als solche genau definiert. In der Regel ist es auch rasch erkennbar, wem dieser Panzer gehört und an wen allfällige Gegenmassnahmen zu richten sind. Im Cyberraum ist diese Zuordnung schwierig.

Als Kernfrage galt lange, ob Cyberaktivitäten physische Schäden bis hin zu Fatalitäten hervorrufen können. Das Überschreiten dieser Schwelle aktiviert, vereinfacht gesagt, im internationalen Kriegsrecht die Möglichkeit zur Verteidigung und den Bündnisfall nach Artikel 5 der Nato.

Ein globales Phänomen

Fehlfunktionen von computergestützten Sensor- und Aktorkomponenten können massive bis fatale Konsequenzen haben. Dies betrifft IoT-Systeme ebenso wie Betriebstechnik, die sogenannte operational technology (OT), die durch nachgerüstete Kommunikationsvernetzung eher ungeplant Teil der IoT-Landschaft wurde. Global demonstrieren gerade in den letzten Jahren Angriffe auf Wasserversorgungen, Krankenhäuser, Pipelines, Industrieanlagen, Kameras und andere Systeme das Schadenspotenzial, das vom Verlust persönlicher und sensitiver Daten bis hin zu ökonomischen Schäden und Fatalitäten reicht.

2010 stellte ein gezielt auf spezifische OT-Systeme entwickelter Computerwurm einen ersten Wendepunkt dar. Mit grossem Aufwand eingeschleust, führte die Schadsoftware Stuxnet in iranischen Nuklearanreicherungsanlagen zu fehlerhaften Betriebsanzeigen in Überwachungssystemen, einer Übersteuerung von Prozessgeschwindigkeiten und schliesslich zur Zerstörung der Zentrifugen.

Im Jahr 2022 hat die Nato Cyberaktivitäten als möglichen Grund zum Aktivieren eines Verteidigungsfalles nach Artikel 5 genannt und konstatiert, dass auch Aktivitäten unterhalb der klassischen kinetischen Schwelle in ihrer Summe als Auslöser gelten können [1]. Dabei werden die oben genannten typischen Grauzonen wie etwa die jeweilige

Au cours de ces derniers mois, la situation géopolitique de la cybersécurité liée à l'Internet des objets (Internet of Things, IoT) s'est gravement détériorée, généralement sans attirer l'attention du public. Pendant longtemps, on a supposé implicitement que les acteurs étatiques tentés de perpétrer des cyberattaques ouvertes contre les infrastructures, en tant que moyen de poursuivre des objectifs stratégiques et militaires, en étaient fortement dissuadés au niveau international.

Cette hypothèse se comprend mieux si l'on se penche sur le contexte, notamment, de l'interaction entre le droit international de la guerre, la stratégie militaire et la cybersécurité. L'avènement de l'informatique et l'interconnexion intégrale des ordinateurs dans la société ont rendu techniquement possible d'agir au-delà des frontières sans avoir à les franchir physiquement. Des moyens techniques permettent également de dissimuler les traces géographiques des activités informatiques, voire de créer de fausses pistes. Il est ainsi difficile, voire impossible, d'identifier les acteurs avec certitude. Il en va autrement dans la manière classique de mener une guerre (guerre cinétique) : un char qui franchit une frontière nationale est clairement reconnaissable en tant que tel, et le franchissement d'une frontière est également précisément défini. En règle générale, il est aussi possible de déterminer rapidement à qui appartient ce char et à qui doivent être adressées d'éventuelles contre-mesures. Dans le cyberespace, ces identifications sont nettement plus difficiles.

La question clé a longtemps été de savoir si les activités cybernétiques pouvaient provoquer des dommages physiques, voire des fatalités. Autrement dit, le dépassement de ce seuil activerait, dans le droit international de la guerre, la possibilité de se défendre et l'engagement de défense mutuelle selon l'article 5 de l'OTAN.

Un phénomène mondial

Des dysfonctionnements de composants de capteurs et d'actionneurs assistés par ordinateur peuvent avoir des conséquences massives, voire fatales. Cela concerne aussi bien les systèmes IoT que la technologie opérationnelle (operational technology, OT), qui est devenue partie intégrante du paysage IoT de manière plutôt imprévue suite à une mise en réseau ultérieure. Ces dernières années, des attaques contre des systèmes d'approvisionnement en eau, des hôpitaux, des pipelines, des installations industrielles, des caméras et d'autres systèmes ont démontré le potentiel en matière de dommages, allant de la perte de données personnelles et sensibles, à des atteintes économiques et des fatalités.

En 2010, un ver informatique développé spécialement pour des systèmes OT spécifiques a marqué un premier tournant. Introduit à grand renfort de moyens dans les installations d'enrichissement nucléaire iraniennes, le malware Stuxnet a entraîné des affichages opérationnels erronés dans les systèmes de surveillance, une

Angriffspunkte
Router werden selten als IoT-Geräte wahrgenommen, sind aber ein Hauptangriffsziel von IoT-Cyberangriffen. Eine typische Schwachstelle sind unsichere Passwörter.

Points d'attaque
Les routeurs sont rarement perçus comme des dispositifs IoT, même s'ils constituent l'une des cibles principales des cyberattaques IoT. Un point faible typique : les mots de passe dont le niveau de sécurité est insuffisant.

Bild | Figure: Compare Fibre

Zuordnung von Akteuren als solche behandelt und von Fall zu Fall beleuchtet. Trotzdem bleibt der Umgang mit Cyberaktivitäten im internationalen Raum eine Herausforderung.

Tatsächlich steht der aktuelle Stand der IoT-Cybersecurity in starkem Kontrast zu dieser Ausgangslage. Mit frei verfügbaren hochentwickelten Scan-Tools, zunehmend unterstützt durch künstliche Intelligenz, werden unsichere Geräte und Schwachstellen identifiziert. Ungeschützte Systeme sind ideale Eintrittspforten in nachgelagerte Zielsysteme wie IT-Infrastrukturen oder Sensorik und Aktorik und ermöglichen Ransomware-Erpressungen, Datenabflüsse, Kryptomining, DDOS-Attacken oder Sabotage.

Gleichzeitig sind unsichere oder gar fehlende Passwörter und offene Ports die Haupteintrittspforten in IoT-Systeme, und ein beachtlicher Teil der eingesetzten IoT-Schadsoftware basiert auf lange bekannter Malware wie Mirai [2].

Auch die Hauptangriffsziele sind seit Jahren unverändert Internet-Router und Kameras. Dennoch werden diese Objekte immer noch weitgehend oder komplett ohne verstärkte Sicherheitsmassnahmen und -instruktionen ausgeliefert. Die jüngste Meldung des Unternehmens Dreamlab, das über 100 000 ungesicherte Schweizer Router identifizierte, ist nur ein Beispiel [3].

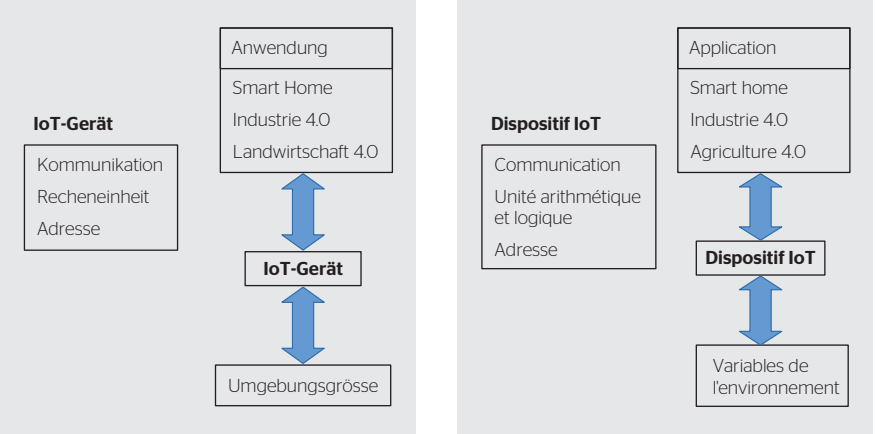
Diesen paradoxen Umgang mit dem IoT zeigte ebenso eine Umfrage des Rogers Cybersecure Catalyst Fellowship Program der Toronto Metropolitan University. Hier waren sich Computer-Sicherheitsexperten mit gewöhnlichen

saturation des vitesses de processus et, finalement, la destruction des centrifugeuses.

En 2022, l'OTAN a cité les activités cybernétiques comme motif possible d'activation d'un cas de défense au sens de l'article 5 et a constaté que des activités inférieures au seuil cinétique classique pouvaient également être considérées en tant que déclencheurs dans leur ensemble [1]. Les zones grises typiques mentionnées ci-dessus, telles que l'identification respective des acteurs, sont traitées en tant que telles et étudiées au cas par cas. La gestion des activités cybernétiques dans l'espace international reste néanmoins un défi.

Dans les faits, l'état actuel de la cybersécurité de l'IoT contraste fortement avec cette situation. Des outils d'analyse sophistiqués disponibles librement, de plus en plus soutenus par l'intelligence artificielle, permettent d'identifier les dispositifs non sécurisés et les points faibles. Les systèmes non protégés représentent des portes d'entrée idéales pour les systèmes cibles en aval, tels que les infrastructures informatiques ou les capteurs et actionneurs, et permettent des extorsions par ransomware, des fuites de données, du cryptomining, des attaques DDOS ou des sabotages.

Parallèlement, des mots de passe peu sûrs, voire inexistants, et des ports ouverts constituent les principales portes d'entrée dans les systèmes IoT, et une part considérable des logiciels malveillants utilisés dans ce domaine se basent sur des malwares connus depuis longtemps, tels que Mirai [2].



Zwei Beispiele einer IoT-Definition (nach [2]). Die Spannweite der Definition eines IoT-Geräts reicht von allgemeinen Funktionsbeschreibungen zu kontextbezogenen Systemen.

Deux exemples de définition de l'IoT (d'après [2]). L'étendue de la définition d'un dispositif IoT va des descriptions générales des fonctions aux systèmes contextuels.

Nutzern einig: Ja, das IoT ist unsicher und wird es vermutlich bleiben, trotzdem wird es, auch persönlich, in den sensibelsten Bereichen eingesetzt [4].

Der unterentwickelte Zustand der IoT-Cybersecurity steht in starkem Kontrast zum Entwicklungsstand des IoT. Zu Generationen von Routern, Druckern und Kameras gesellen sich Smart-Home-Geräte genauso wie Schwärme von RoboBees, also künstlicher Bienen **(Einstiegsbild)**. Der Einsatz der Künstlichen Intelligenz auf IoT-Geräten und die Eignung von Verschlüsselungsmethoden für das beginnende Zeitalter des Quantumcomputings sind bereits jetzt Kriterien in Beschaffungsprozessen.

Der widersprüchliche Stand der IoT-Cybersecurity

Der Siegeszug digitaler Technologien in allen Ebenen der Gesellschaft hat zuvor bestehende klare Einteilungen verschoben. Dies ist nur wenigen Anwendern bewusst. Für Cyber-Angreifer aller Art ist dies praktisch: Mit der weiten und unregulierten Verbreitung von IoT-Geräten steht eine riesige Angriffsfläche bereit, die weitestgehend von ahnungslosen Nutzern betrieben wird. Nutzer, die den Schutz ihrer Geräte verbessern oder gar nur beurteilen wollen, stehen vor einer schwierigen Aufgabe. Oft kennen nicht einmal die Anbieter alle relevanten Informationen, wie etwa Datenflüsse oder Fernzugriffe, im Detail. Zudem erschweren fehlende Standards eine Bewertung: Wie sicher ist ein Produkt nun im Vergleich? Ist es sicher genug? Wie genau ist sicher definiert und braucht es die gleiche Definition für verschiedene Zwecke?

Für IoT-Hersteller ist eine höhere Sicherheit ein Dilemma. Solange sie für Kunden mangels spezifischer Standards weder prüf- noch vergleichbar ist, resultiert bei womöglich höheren Kosten allenfalls nur ein komplizierter zu bedienendes Produkt. Aus Wettbewerbssicht werden Anbieter ohne verbindliche und einheitliche Regulierung kaum motiviert, Geräte sicherer zu machen.

Die Gesetzesgebung greift die Thematik zunehmend auf. Verschiedene Gesetze, Standards und Richtlinien sind inzwischen in Kraft getreten oder in der Vernehmlassung. Eines der weitreichendsten Gesetze ist der in

De même, les routeurs Internet et les caméras restent les principales cibles des attaques depuis des années. Pourtant, ces objets sont toujours en grande partie ou complètement livrés sans mesures ni instructions en matière de sécurité renforcée. La récente annonce de l'entreprise Dreamlab, qui a identifié plus de 100 000 routeurs suisses non sécurisés, n'en est qu'un exemple [3].

Cette manière paradoxale de procéder avec l'IoT a également été mise en évidence par une enquête du Rogers Cybersecure Catalyst Fellowship Program de l'Université métropolitaine de Toronto. Les experts en sécurité informatique étaient d'accord avec les utilisateurs ordinaires : l'IoT n'est pas sûr et le restera probablement, mais il est tout de même utilisé, y compris à titre personnel, dans les domaines les plus sensibles [4].

L'état de sous-développement de la cybersécurité de l'IoT contraste fortement avec le niveau de développement de l'IoT. Aux générations de routeurs, d'imprimantes et de caméras s'ajoutent des appareils smart home tout comme des essaims de RoboBees, ou abeilles artificielles (figure de titre). L'utilisation de l'intelligence artificielle sur les dispositifs IoT et l'adéquation des méthodes de cryptage pour l'ère naissante de l'informatique quantique constituent déjà des critères dans les processus d'achat.

L'état contradictoire de la cybersécurité de l'IoT

Le succès des technologies numériques à tous les niveaux de la société a chamboulé des classifications qui étaient claires auparavant. Peu d'utilisateurs en sont conscients. Ceci est pratique pour les cyberattaquants de toutes sortes : avec la diffusion étendue et non réglementée des dispositifs IoT, une énorme surface d'attaque est disponible, exploitée en grande partie par des utilisateurs qui ne se doutent de rien. Et les utilisateurs qui souhaitent améliorer la protection de leurs appareils, ou même simplement l'évaluer, sont confrontés à une tâche difficile. Souvent, les fournisseurs ne connaissent eux-mêmes pas en détail toutes les informations pertinentes telles que les flux de données ou les accès à distance. De plus, l'absence de normes rend l'évaluation difficile : à quel point

Bild | Figure : Monika Freunek [2]

diesem Jahr erwartete Cyber Resilience Act der EU, der klassische IT- ebenso wie IoT- und OT-Geräte abdeckt. Mit einer Übergangszeit von drei Jahren wird dieses Gesetz die IoT-Produktlandschaft beträchtlich verändern und Hersteller wie Anbieter in die Pflicht nehmen. In der Schweiz stehen allgemein mit dem neuen Informationssicherheitsgesetz (ISG) zunächst Einrichtungen des Bundes und kritische Infrastrukturen im Fokus. Implikationen von Anforderungen des Datenschutzes an IoT-Systeme, wie in der Schweiz beim total revidierten Datenschutzgesetz (DSG), das ohne Übergangsfrist seit 2023 gilt, werden dabei oft übersehen. Gerade IoT-Geräte mit ihrem häufig globalisierten Datenfluss, geringem Sicherheitsniveau und ihrer oft niedrigen Sichtbarkeit im Netzwerk benötigen hier besondere Aufmerksamkeit. Nicht immer ist die eingesetzte Technologie allen Beteiligten in vollem Umfang bewusst.

Unterschiedliche Definitionen erschweren die Standardisierung

Weltweit unterscheiden sich die gesetzlichen Lösungsansätze deutlich. Allein die Definition regulierter Geräte reicht von hochgradig detaillierten Komponentenbeschreibungen in eng umrissenen Anwendungsfällen bis zu technologieunabhängigen Anforderungen an Handlungen rund um Informationen. So wäre nach beiden Definitionen im nebenstehenden **Bild** ein Smart Meter ein IoT-Gerät. Ein Laptop würde unter die allgemeine Definition fallen, ein Smartphone unter beide – einige IoT-Cybersecurity-Richtlinien schliessen diese Geräte jedoch explizit aus, obwohl mindestens Smartphones dank Sensorik und Betriebssystem sowohl klassische IT- als auch IoT-Geräte sind.

Während der detaillierte Ansatz den Vorteil der Überprüfbarkeit bietet, beschränkt er zugleich die Reichweite der Sicherheitsstandards und ist kaum wirksam. Im anderen Ansatz erschwert die fehlende Schärfe die Überprüfbarkeit, aber auch die Anleitung zur Umsetzung. Betreiber stehen vor Unklarheiten und dem Risiko, es allenfalls darauf ankommen lassen zu müssen. Im Falle eines Schadens ist dann die Frage, wie sich ein nicht definiertes oder technisch nicht realisierbares Sicherheitsniveau bewerten lässt – reicht es, dass alle gleich unsicher sind? Müssen unsichere Systeme aus dem Betrieb genommen werden, und falls ja, nach welchen Kriterien? Hier zeigt sich die Herausforderung, die Realitäten aus Legislative, Forschung und Praxis rechtzeitig miteinander in einen Dialog zu bringen.

Insgesamt entwickelt sich die IoT-Cybersecurity zunehmend als Wirtschafts-, Wettbewerbs- und Standortfaktor. Für Unternehmer werden Haftungsfragen, aber auch die Erhaltung der Wettbewerbsfähigkeit und die betriebliche Zuverlässigkeit des Standortes angesichts steigender Cyberangriffe relevant. Für Hersteller von IoT-Produkten zeichnet sich ab, dass international vermehrt Sicherheit eingefordert wird.

Aktuell gilt als Richtannahme, dass ein IoT-System vermutlich unsicher und ebenso wahrscheinlich bereits oder bald gehackt ist. Obwohl die Herausforderungen IoT-spezi-

un produit est-il sûr en comparaison d'un autre ? Est-il suffisamment sûr ? Quelle est la définition exacte de la sécurité, et cette définition doit-elle être la même pour différents usages ?

Pour les fabricants IoT, une sécurité accrue représente un dilemme. Tant qu'elle n'est ni vérifiable ni comparable pour les clients en raison de l'absence de normes spécifiques, il n'en résulte qu'un produit plus compliqué à utiliser, avec des coûts éventuellement plus élevés. Du point de vue de la concurrence, sans réglementation contraignante et uniforme, les fournisseurs ne sont guère incités à rendre leurs appareils plus sûrs.

La législation s'occupe de plus en plus de cette thématique. Diverses lois, normes et directives sont désormais entrées en vigueur ou sont en cours de consultation. L'une des lois les plus ambitieuses est le Cyber Resilience Act de l'UE, attendu cette année, qui couvre aussi bien les appareils IT classiques que les dispositifs IoT et OT. Avec une période de transition de trois ans, cette loi modifiera considérablement le marché de l'IoT et mettra les fabricants et les fournisseurs face à leurs responsabilités. En Suisse, la nouvelle loi sur la sécurité de l'information (LSI) se concentre d'abord sur les institutions fédérales et les infrastructures critiques. Les implications des exigences relatives à la protection des données pour les systèmes IoT, comme avec la loi sur la protection des données (LPD) totalement révisée, entrée en vigueur en Suisse en 2023 sans période de transition, sont souvent négligées. Or, ce sont justement les dispositifs IoT, avec leur flux de données souvent globalisé, leur faible niveau de sécurité et leur visibilité fréquemment réduite dans le réseau, qui nécessitent une attention particulière à cet égard. Toutes les parties concernées ne sont pas toujours pleinement conscientes de la technologie utilisée.

Des définitions différentes compliquent la standardisation

À l'échelle globale, les approches de solutions légales varient considérablement. Rien que la définition des dispositifs réglementés va de descriptions de composants très détaillées dans des cas d'application étroitement définis, à des exigences indépendantes de la technologie pour les actions autour des informations. Ainsi, selon les deux définitions de la figure ci-contre, un compteur intelligent serait un dispositif IoT. Un ordinateur portable répondrait à la définition générale, un smartphone aux deux – certaines directives en matière de cybersécurité de l'IoT excluent toutefois explicitement ces appareils, bien que les smartphones, au moins, soient à la fois des appareils informatiques classiques et des dispositifs IoT du fait de leurs capteurs et de leur système d'exploitation.

Alors que l'approche détaillée présente l'avantage d'être vérifiable, elle limite en même temps la portée des normes de sécurité et n'est guère efficace. Dans l'autre approche, le manque d'acuité rend difficile la vérifiabilité, mais aussi les instructions de mise en œuvre. Les exploitants sont confrontés à un manque de clarté et au risque de devoir

fischer Cybersecurity noch beträchtlich sind, zeigen die jüngsten Entwicklungen, dass die IoT-Sicherheit langsam erwachsen wird. Entsprechend heisst es, Sicherheitshausaufgaben zügig umzusetzen, die aktuell hochdynamischen Entwicklungen aufmerksam zu verfolgen, und auch für den Fall eines Ausfalls von IoT-Geräten vorbereitet zu sein. Frei nach dem bekannten Rat: Klüger dran, Notfallplan.

Referenzen | Références

[1] Sarah Wiedemar, Center for Security Studies (CSS), ETH Zürich, Nato and Article 5 in Cyberspace, CSS Analyses in Security Policy, May 2023.
[2] M. Freunek, A. Rombos, «Classification of cyber attacks on IoT and ubiquitous computing devices», arXiv, Dezember 2023. arXiv:2312.00686 [cs.CR]
[3] Dreamlab, «Swiss Cyberspace: 100 000 Unprotected Routers Exposed Online». 16. Februar 2024. dreamlab.net/de/news/artikel/swiss-cyberspace-100000-unprotected-routers-exposed-online
[4] M. Freunek, «The Internet of Things exposes us all to the biggest cyber threats», Toronto Star, 20. März 2023. www.thestar.com/opinion/the-internet-of-things-exposes-us-all-to-the-biggest-cyber-threats/article_6448955a-04bb-5bad-ae02-72425e405c0a.html

Autorin | Auteure

Dr.-Ing. **Monika Freunek** ist Geschäftsführerin der Lighthouse Science Consulting and Technologies Inc., Kanada, und Dozentin für Cybersecurity an der Toronto Metropolitan University.

Dr **Monika Freunek** est directrice de Lighthouse Science Consulting and Technologies Inc., au Canada, et chargée de cours en cybersécurité à l'Université métropolitaine de Toronto.

→ Lighthouse SCT, New Brunswick, Canada
→ monika.freunek@lighthouse-sct.com

éventuellement s'y résoudre. En cas de dommage, la question est alors de savoir comment évaluer un niveau de sécurité non défini ou techniquement irréalisable – suffit-il que tous les appareils disposent du même faible niveau de sécurité ? Les systèmes peu sûrs doivent-ils être retirés de l'exploitation et, si tel est le cas, selon quels critères ? C'est là qu'apparaît le défi consistant à initier à temps le dialogue entre les réalités du législatif, de la recherche et de la pratique.

Dans l'ensemble, la cybersécurité de l'IoT se développe de plus en plus en tant que facteur économique, concurrentiel et géographique. Pour les entrepreneurs, autant les questions relatives à la responsabilité qu'au maintien de la compétitivité et à la fiabilité opérationnelle du site deviennent pertinentes face à l'augmentation des cyberattaques. Pour les fabricants de produits IoT, il semble que la sécurité soit de plus en plus demandée au niveau international.

Actuellement, on part du principe qu'un système IoT n'est vraisemblablement pas sûr et qu'il est probable qu'il soit déjà, ou bientôt, piraté. Bien que les défis de la cybersécurité spécifique à l'IoT soient encore considérables, les derniers développements montrent que la sécurité de l'IoT arrive lentement à maturité. Il s'agit donc de mettre rapidement en œuvre les tâches en matière de sécurité, de suivre attentivement les développements actuels, qui sont très dynamiques, et d'être préparé à l'éventualité d'une panne des dispositifs IoT. Selon le dicton bien connu : « Mieux vaut prévenir que guérir ».