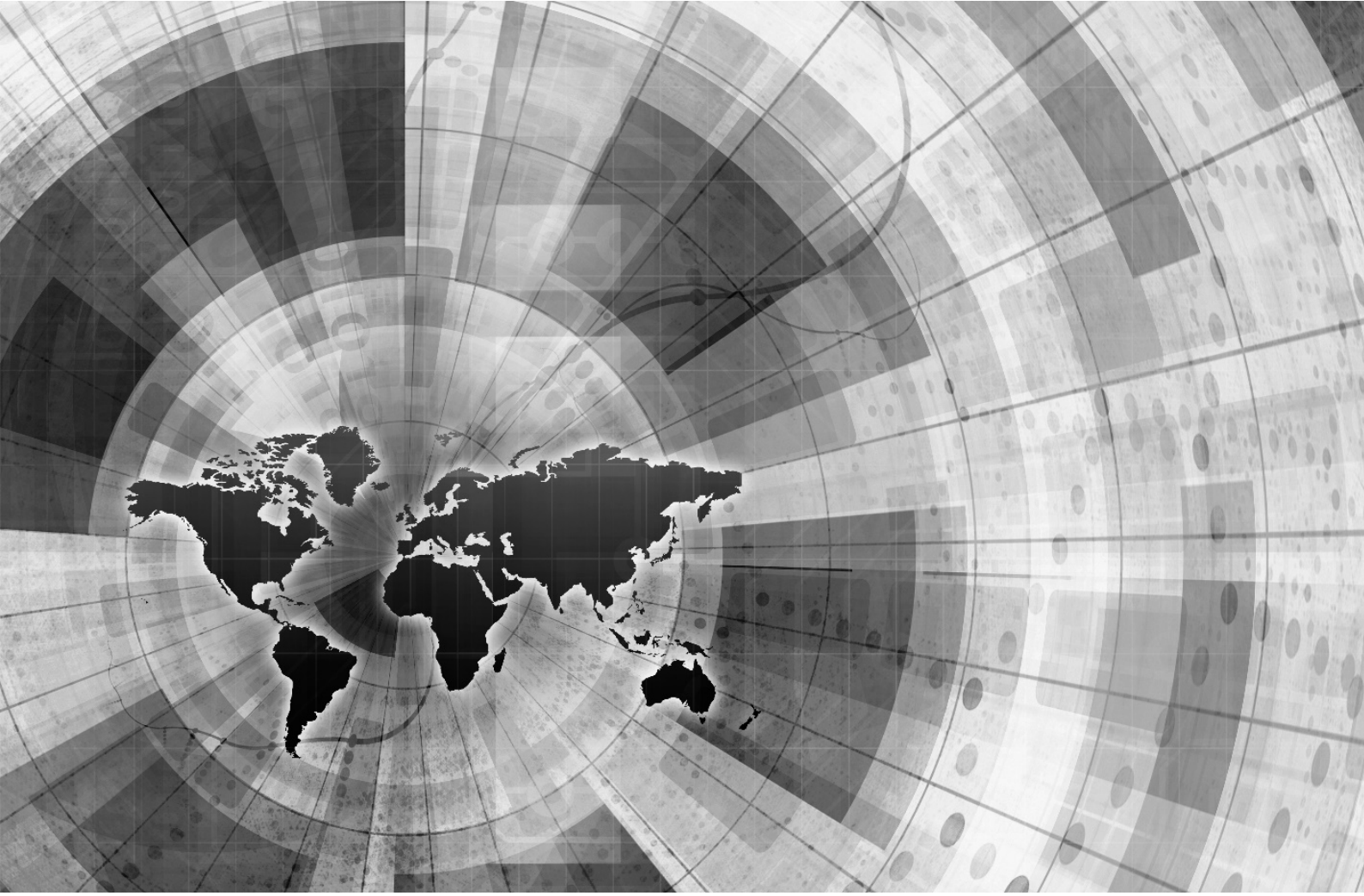


Supply Chain Security

Analyse et mesures visant à sécuriser la chaîne d'approvisionnement numérique

Groupe de travail Supply Chain Security de la
Commission Cybersécurité d'ICTswitzerland

Septembre 2019

ICTSWITZERLAND

Mentions légales

ICTswitzerland
Aarbergergasse 30
CH - 3011 Berne

Auteurs:
Dr Stefan Frei, Christof Jungo[1], Daniel Busch[2], Dr Raphael Reischuk

Remarque:
Le rapport traduit principalement l'avis du groupe de travail. Le rapport ne reflète toutefois pas forcément les positions des organisations des membres.

Suivi:
Groupe de travail Supply Chain Security de la Commission Cybersécurité d'ICTswitzerland

Dr Stefan Frei	Cyber Security Principal, Accenture Responsable du groupe de travail Supply Chain Security d'ICTswitzerland
Umberto Annino	Head Security Governance, SIX Group
Markus Bischof	Director Europe Security & Trust Organization, Cisco Systems GmbH
Tobias Ellenberger	Membre du conseil d'administration, Swiss Cyber Expert Chief Operating Officer, Oneconsult AG
Dr Jon Albert Fanzun	Envoyé spécial pour la politique étrangère et de sécurité relative au cyberspace, DFAE
Christophe Gerber	Head of Business Line, ELCA Informatique SA
Christian Grasser	Directeur, asut
Thomas Holderegger	Head of Security IT, UBS AG
Andreas Kaelin	Directeur d'ICTswitzerland
Uwe Kissmann	Managing Director Cyber Security Services EALA, Accenture Président de la Commission «Cyber Security» d'ICTswitzerland
Arié Malz	Conseiller spécial TIC et passage au numérique, Secrétariat général du département fédéral des finances
Dr Raphael Reischuk	Head of Cyber Security Services, Zühlke Engineering AG Vice-président de la Commission «Cyber Security» d'ICTswitzerland
Gérald Vernez	Délégué à la cyberdéfense, Département fédéral de la défense de la protection de la population et des sports, DDPS
Nicole Wettstein	Responsable du programme prioritaire Cybersecurity, SATW

[1] SecIntel GmbH
[2] Symantec (Deutschland) GmbH

Résumé

Internet relie de plus en plus les hommes et les machines et a, aujourd'hui déjà, changé nos vies de façon durable. L'intégrité et la sécurité des produits des secteurs traditionnels sont contrôlés à certains niveaux avant l'autorisation de mise sur le marché (par exemple dans le domaine de la mobilité, de l'alimentation, des médicaments, etc.), mais la qualité et la sécurité de nombreux produits numériques n'est souvent pas suffisamment contrôlée, pour de nombreuses raisons. La sécurité actuelle de la chaîne d'approvisionnement (Supply Chain) des produits numériques est souvent insuffisante et sape ainsi les mesures de sécurité existantes. De plus, les décideurs ne sont souvent pas en mesure de prendre des décisions durables faute d'informations fondées et transparentes.

Par le passage au numérique croissant, l'ignorance du niveau de sécurité des produits utilisés peut mener à des menaces critiques. Si des produits n'ayant pas subi un contrôle complet sont utilisés dans des infrastructures critiques, les menaces peuvent se multiplier jusqu'à mettre en danger l'approvisionnement de la société dans des domaines tels que l'électricité, les soins de santé, la mobilité et la protection physique. Les risques qui les accompagnent sont souvent abstraits et évoluent insidieusement et ont ainsi à peine été pris en compte pendant longtemps, s'accumulant continuellement jusqu'à aujourd'hui.

Le groupe de travail Supply Chain Security analyse la façon d'aborder les risques technologiques dans d'autres secteurs (par ex. l'électricité), puis identifie et documente sur cette base des mesures nécessaires pour un passage au numérique en toute sécurité. Les questions suivantes sont entre autres abordées:

- Quels sont les plus grands risques de la société numérique et où se situent-ils?
- À quoi ressemblent des scénarios d'attaque critiques, qui sont les agresseurs?
- À quoi pouvons et devons-nous faire attention ou que pouvons et devons-nous entreprendre aujourd'hui déjà en tant que société ou secteur?
- Quelles mesures de sécurisation de la chaîne d'approvisionnement numérique sont nécessaires et utiles?

La société doit désormais empêcher les erreurs connues et évitables afin que les opportunités offertes par le passage au numérique l'emportent sur les risques.

Contenu

Mentions légales 2

Résumé 3

Situation initiale: la société numérique 5

- Développement et cyberrisques 5
- Cybercriminels et acteurs étatiques 5
- Brouillard numérique 7

La chaîne d'approvisionnement des produits numériques 10

- Origine et fabricant 10
- Comparaison des chaînes d'approvisionnement traditionnelle et numérique 10
- Intégrité de la chaîne d'approvisionnement 11
- Sabotage et espionnage 12
- Matériel informatique compromis 13

Technologie et histoire de l'innovation 15

- L'introduction d'innovations de rupture 15
- Leçons pour la société numérique 16

Perspectives et mesures 18

- La responsabilité du fabricant et du fournisseur 18
- Exigences applicables aux produits 19
- Laboratoire de cybertests indépendant 19
- Vision pour une Suisse digitale 20

Conclusion 21

Situation initiale: la société numérique

Développement et cyberrisques

La société connectée devient constamment et rapidement de plus en plus complexe en raison du nombre croissant de nouvelles interactions entre les personnes, les machines, les services et divers processus de rétroaction. De nouveaux risques pour les infrastructures critiques voient le jour, en particulier en raison des dépendances vis-à-vis du matériel et des logiciels ainsi que lors de l'achat de prestations (directes ou déléguées)[3]. Des incidents de sécurité peuvent être déclenchés par des dysfonctionnements ou des manipulations de composants matériels ou logiciels, mais aussi par hasard en raison d'un manque de qualité de la conception ou du développement des composants ou par des attaques ciblées.

Si des produits numériques présentant des failles de sécurité sont commercialisés, ces points faibles peuvent avoir des répercussions pendant des dizaines d'années. Des appareils fixes dans les systèmes de contrôle industriels ou domestiques sont par exemple concernés, et les infrastructures critiques ne font pas exception.

Les caractéristiques d'un système complexe et connecté ne peuvent plus être déduites par l'analyse isolée du comportement de composants individuels. Des propriétés nouvelles et parfois surprenantes des systèmes apparaissent, telles que l'organisation autonome ou l'émergence[4]. Une petite perturbation locale, déclenchée par hasard ou par un dysfonctionnement, peut avoir des répercussions imprévisibles et à distance.

Exemples:

- Influence de masse sur des sociétés dans leur ensemble par les médias sociaux[5].
- Une application de suivi de fitness révèle la position de bases militaires secrètes[6].

Cybercriminels et acteurs étatiques

Le passage au numérique est suivi et exploité par des agresseurs de tous types. Dans un passé récent, des attaques se sont multipliées pour atteindre des objectifs politiques en exploitant des vulnérabilités de la société numérique. L'histoire nous a enseigné que les services secrets et les criminels s'approprient toujours très vite les nouvelles technologies.

[3] «Par infrastructures critiques, on entend les processus, les systèmes et les installations qui sont essentiels pour le fonctionnement de l'économie ou le bien-être de la population.» (Par ex. l'approvisionnement en électricité et en eau) Définition de l'OFPP: https://www.babs.admin.ch/fr/aufgabenbabs/ski.html
[4] Système complexe adaptatif
https://fr.wikipedia.org/wiki/Système_complexe_adaptatif
[5] Comment les réseaux sociaux s'emparent de la société
https://www.nzz.ch/feuilleton/medien/wie-die-sozialen-netzwerke-die-gesellschaft-praegen-ld.1380183
[6] Fitness tracking app Strava gives away location of secret US army bases
https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

De tout temps, les États et les services de renseignement se sont impliqués dans l'espionnage et le sabotage, et ces tactiques sont de plus en plus présentes dans les stratégies d'attaque et de défense militaires[7].

Illustration 1: Menaces dans le système complexe de la société numérique – déclenchées par hasard ou par des attaques ciblées de certains acteurs.

Pour l'appréciation des vulnérabilités critiques, le passage de la société au numérique doit être considéré du point de vue des agresseurs. Les questions suivantes contribuent à adopter la perspective correcte:

- Comment un agresseur expérimenté peut-il exercer une influence maximale et obtenir la persistance la plus importante tout en ayant la probabilité la plus faible d'être détecté?

- Comment un agresseur procède-t-il lorsque son objectif de base est très bien sécurisé?

L'histoire criminelle et militaire nous montre que les agresseurs qui sont parvenus à leurs fins identifiaient souvent les points les plus faibles. L'attaque est menée là où le défenseur l'attend le moins. Le fait de compromettre des produits numériques avant leur livraison, c'est-à-dire pendant leur conception, leur fabrication ou dans la chaîne d'approvisionnement répond donc parfaitement à ce critère d'attaque.

Un certain nombre d'États renforcent actuellement leurs cybercompétences offensives et défensives. À la différence des cybercriminels et des autres agresseurs, ces États peuvent: . .

- . . . obtenir un accès direct à des parties critiques de l'infrastructure d'Internet («Internet Backbone»),

[7] Luiijf, E., Besseling, K. and de Graaf, P. (2013) 'Nineteen national cyber security strategies', Int. J. Critical Infrastructures, Vol. 9, Nos. 1/2, pp.3–31.

- . . . contraindre légalement des fournisseurs de services ou des fabricants à collaborer ou à procéder à de la surveillance,

- . . . surveiller le trafic Internet de façon systématique et à grande échelle.

Les agresseurs étatiques disposent de ressources supérieures à la moyenne et d'un horizon à long terme pour atteindre un but par le biais de plusieurs canaux d'attaque et sur de longues périodes sans qu'on les découvre. La persistance et la possibilité d'attaquer en cas de besoin sont les principaux objectifs. Les activités de l'agresseur comprennent l'introduction cachée de malware et de backdoors (portes dérobées) dans les équipements informatiques et les logiciels des systèmes cibles d'autres pays (ou de concurrents).

La cybersécurité ne devrait pas se limiter aux logiciels et à la sécurité réseau, mais bien inclure l'intégrité et la sécurité du matériel et de ses composants ainsi que le facteur humain. En définitive, la plupart des composants sont installés, configurés et utilisés par des humains.

Exemples:

- Les Israéliens et les Américains auraient développé ensemble le ver informatique Stuxnet, qui a paralysé une grande partie des installations nucléaires iraniennes[8].

- Après avoir compromis le système du fabricant d'ordinateurs ASUS, un malware a contaminé les systèmes des clients ASUS par le biais de la fonction de mise à jour automatique [9].

- Exemples des cyberattaques significatives ayant visé des autorités gouvernementales ainsi que des entreprises des secteurs de la défense et de la haute technologie[10].

Brouillard numérique

Les attaques au sein de la chaîne d'approvisionnement ne peuvent en principe être ni exclues ni totalement empêchées. Une protection efficace contre de telles menaces contre l'environnement numérique est aujourd'hui quasiment inexistante. Chaque type d'attaque continuera à proliférer facilement tant que les éléments suivants continueront d'être vrais:

- La compromission d'un produit est impossible à détecter.

[8] Israël et les États-Unis se cacheraient derrière l'attaque informatique https://www.nzz.ch/iran_israel_usa_stuxnet-1.9110811
[9] Des centaines de milliers d'ordinateurs Asus infectés par un virus https://www.tagesanzeiger.ch/digital/computer/hunderttausende-von-asuscomputern-mit-virus-infiziert/story/19690172
[10] Significant Cyber Incidents Since 2006 (incidents significatifs depuis 2006)https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents

- Des critères de qualité minimaux ne peuvent pas être imposés aux fabricants (et à leurs sous-traitants).

- L'entretien de l'infrastructure n'est pas assuré parce que les mises à jour de sécurité ne sont pas diffusées de façon fiable.

Cette situation n'est plus acceptable compte tenu de la dépendance croissante vis-à-vis des produits numériques. En raison de moyens de détection insuffisants, il faut partir du principe qu'aujourd'hui déjà, des parties de l'infrastructure critique de la Suisse sont compromises.

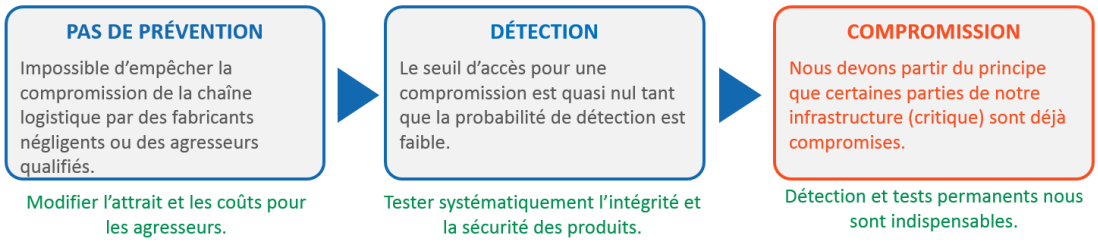


Illustration 2: Si la qualité et la sécurité des produits numériques ne sont ni exigées ni vérifiées, nous devons supposer qu'il existe un grand nombre de produits compromis, y compris dans les fonctions critiques.

Les exemples suivants du domaine de la chaîne d'approvisionnement montrent les conséquences de la compromission en raison d'une détection insuffisante:

- **Machines à écrire IBM | Union soviétique 1970**
  L'Union soviétique compromet les machines à écrire IBM avant leur livraison à l'ambassade américaine à Moscou. Pendant environ 8 ans, les Soviétiques ont pu lire les textes dactylographiés de l'ambassade américaine[11].

- **Terminaux de paiement (PDV) | Cybercriminels 2008**
  Des terminaux de paiement compromis en Europe exfiltrent des informations de cartes de crédit et des mots de passe par implant GSM directement vers des cybercriminels à l'étranger[12].

- **Boîte à outils de la NSA | États-Unis 2013**
  Des logiciels malveillants et des implants dans le matériel informatique des processeurs de Cisco, Dell, Juniper, Hewlett-Packard (HP) et Huawei sont installés par les services secrets américains de la NSA[13].

[11] Opération GUNMAN https://www.cryptomuseum.com/covert/bugs/selectric/
[12] Chip and pin scam 'has netted millions from British shoppers' https://www.telegraph.co.uk/news/uknews/law-and-order/3173346/Chip-and-pin-scam-has-netted-millions-from-British-shoppers.html
[13] La boîte à outils secrète de la NSA https://www.spiegel.de/netzwelt/netzpolitik/neue-dokumente-der-geheime-werkzeugkasten-der-nsa-a-941153.html

- **BlackIOT, High Wattage Botnet | 2018**
  Un réseau zombie avec des appareils de climatisation et de chauffage IoT (Internet des objets) compromis peut menacer l'approvisionnement en électricité d'une région[14].

Même si la sécurité absolue n'existe pas (aussi bien dans le monde numérique que réel), des mesures appropriées doivent être prises, pour: . .

- . . . augmenter la barrière à l'entrée, la complexité et les coûts pour les agresseurs,
- . . . réduire la probabilité de réussite des attaques,
- . . . permettre la détection des attaques et l'identification des agresseurs,
- . . . imposer une obligation en matière de qualité et de sécurité aux fabricants et exploitants des produits.

Autrement dit, cela signifie d'une part qu'un agresseur ne peut plus être en mesure de mettre en danger la sécurité du passage au numérique sans risques considérables pour lui-même. D'autre part, cela implique que les fabricants doivent assumer la responsabilité pour la sécurité de leurs produits numériques.

[14] BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid
https://www.usenix.org/conference/usenixsecurity18/presentation/soltan

La chaîne d'approvisionnement des produits numériques

Comme précédemment mentionné, la sécurisation de la chaîne d'approvisionnement revêt une importance particulière et est par conséquent étudiée de près dans les éléments suivants.

Illustration 3: Chaîne d'approvisionnement de produits numériques et de composants, depuis la conception du matériel informatique jusqu'à l'utilisation chez le client final en passant par l'intégration et l'envoi.

Origine et fabricant

La plupart des infrastructures numériques sont issues d'un grand nombre de fournisseurs de différentes origines. Les composants ainsi que les sous-composants sont habituellement fabriqués dans une chaîne d'approvisionnement complexe qui, du fait même de cette complexité, est à peine compréhensible et impossible à contrôler. Avec la diffusion croissante des produits numériques, la complexité croissante de la chaîne d'approvisionnement représente une menace considérable pour la société numérique.

Comparaison des chaînes d'approvisionnement traditionnelle et numérique

L'approche traditionnelle de la sécurisation de la chaîne d'approvisionnement repose sur l'hypothèse que la menace la plus importante réside dans la fabrication. Cette approche doit être élargie dans le cas des produits numériques:

- avec la complexité croissante des processeurs et des puces, la menace se déplace en direction de la conception des puces et des composants. Cela comprend les environnements de développement, y compris les logiciels et les outils, qui servent à la conception des puces.

- Les produits traditionnels on reliés au réseau ne subissent quasiment aucune modification après leur livraison. Par contre, des dysfonctionnements intégrés dans les produits mis en réseau peuvent être activés également après la livraison. Un dysfonctionnement ou une porte dérobée peuvent tout aussi bien être activés par le biais d'une mise à jour.

- Contrairement aux produits non reliée au réseau, les mises à jour de sécurité du fabricant sont nécessaires. Cela s'applique en particulier pendant la totalité de la durée de vie du produit numérique.

- Les produits traditionnels peuvent dans la plupart des cas être contrôlés par une inspection visuelle. L'intégrité des produits numériques ne peut souvent être évaluée qu'à l'aide de lourdes procédures de test.

- Les produits traditionnels ne peuvent quasiment pas être manipulés de manière isolée du fait de l'absence de possibilité de les mettre en réseau. Tous les produits d'une série sont identiques. Les produits mis en réseau par contre, peuvent être manipulés de façon isolée à distance. Les procédures de test sont par conséquent plus complexes.

- Une poignée de fabricants dominent le marché de certains types de produits ou sous-composants numériques (par ex. les processeurs, les puces WLAN, les adaptateurs, etc.). Cela induit une concentration d'incitations pour les agresseurs. Une attaque sur un fabricant dominant a des conséquences à l'échelle mondiale.

Intégrité de la chaîne d'approvisionnement

En cas d'attaque par le biais de la chaîne d'approvisionnement, les composants sont déjà compromis ou manipulés avant leur livraison à l'utilisateur final. Cela peut déjà se produire lors de la conception et du développement des puces, lors de la fabrication ou de l'intégration des composants ou pendant le transport jusque chez l'utilisateur final. La manipulation pendant l'exploitation, par ex. par la fourniture d'un firmware compromis, doit également être prise en compte. L'intégrité des objets numériques à livrer est particulièrement menacée par des accès et des portes dérobées non documentés ou des dysfonctionnements implantés.

Globalement nous distinguons les types suivants de menaces:

(A) Attaque ciblée	(B) Attaque opportuniste
Un seul produit compromis entraîne des répercussions critiques sur l'organisation cible. La compromission ciblée de produits définis d'une organisation ou d'un secteur permet d'accéder à un environnement clairement identifié et d'avoir une influence sur celui-ci. • Équipement de réseau spécial (ISP, GSM, etc.) • Systèmes de contrôle industriels (ICS) • Internet industriel des objets (IIdO) • Produits spécifiques à un secteur (militaire, énergie, médical)	**Seule une large diffusion du produit compromis devient critique.** La compromission de biens de consommation numériques accessibles à tous destinés aux particuliers et/ou industriels permet d'avoir une influence sur une grande partie des produits. • Ordinateurs / périphériques d'ordinateurs • Compteurs intelligents, grille-pain, téléviseurs, machines à laver • Systèmes domotiques • IdO, capteurs • Par ex. Réseau zombie Mirai, attaques DDoS

Les frontières entre ces types de menaces sont floues.

Sabotage et espionnage

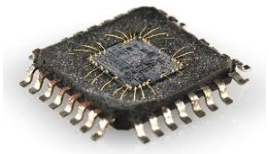
Certains services de renseignement mettent en place de plus en plus de mesures telles que des Kill Switches (interrupteurs d'urgence) pour préparer un sabotage de systèmes étrangers en cas de besoin. Des fonctionnalités de ce type peuvent se manifester par exemple sous forme de vulnérabilités de logiciels ou de comptes d'accès installés définitivement à de prétendues fins de maintenance. La partie attaquée ne peut quasiment pas attribuer clairement des dysfonctionnements de ce type à une action ciblée d'un adversaire spécifique. Il est donc presque impossible de prouver clairement le sabotage.

Matériel informatique compromis

Le matériel informatique peut lui aussi être muni de fonctionnalités cachées, livrées avec celui-ci et pouvant être activées à distance en cas de besoin. Les produits numériques sans dispositifs de saisie (souris, écrans, etc.) ne fonctionnent souvent pas comme des ordinateurs en réseau (par ex. les appareils de l'IdO tels que les grille-pains intelligents). Dans ce cadre, ce sont justement ces produits numériques qui sont souvent utilisés avec du matériel et des logiciels insuffisamment sécurisés au sein de réseaux eux-mêmes la plupart du temps non protégés. Des attaques visant tant le firmware que les équipements matériels sont possibles et très attrayantes pour les agresseurs.

De par le monde, chaque année, plus de 5'000 nouvelles puces sont développées dans d'innombrables sociétés comptant des centaines de milliers d'ingénieurs. D'un point de vue statistique, il y a par conséquent suffisamment de collaborateurs ayant les capacités et l'accès nécessaire pour compromettre les puces déjà à l'étape de la conception. Cela peut se produire en raison de motivations personnelles ou du fait de pressions / chantages[15].

Le matériel informatique compromis permet entre autres:



- l'exfiltration de données sensibles, par ex. par le biais de «Covert Channels» (canaux dissimulés),
- l'accès et le contrôle à distance de systèmes,
- la manipulation des fonctionnalités, par ex. la génération de résultats incorrects,
- la diffusion de logiciels compromis et l'utilisation forcée d'algorithmes peu sûrs,
- la destruction physique sur commande (Kill Switch).

La protection et l'élimination de matériel peu sûr peuvent être très coûteuses et nécessiter beaucoup de temps, une mise à jour du logiciel n'étant dans de nombreux cas pas suffisante (par ex. le remplacement de tous les compteurs intelligents dans une ville, voire une région).

Sans contrôle qualité fiable des produits numériques, nous devons partir du principe que des composants compromis sont déjà en service aujourd'hui. D'autres composants compromis viendront s'y ajouter régulièrement, parfois dans des fonctions critiques.

[15] Compromised By Design?
https://www.brookings.edu/wp-content/uploads/2016/06/Villasenor_HW_Security_Nov7.pdf

Le Général Michael Hayden, ancien directeur de la CIA et de la NSA a exprimé cette problématique comme suit: *«Frankly, it's not a problem that can be solved, this is a condition that you have to manage.» («Franchement, il ne s'agit pas d'un problème qu'il est possible de résoudre. C'est une situation qu'il faut gérer.»)* [15]

Technologie et histoire de l'innovation

Y a-t-il des enseignements de l'histoire qui nous aident à mieux comprendre le développement de la cybersécurité de la société numérique ou à la faire avancer?

L'introduction d'innovations de rupture

Lors de l'introduction d'une innovation (par ex. l'automobile, l'aviation), la sécurité est secondaire car l'expérience et les normes de sécurité manquent encore. Avec la diffusion croissante, les incidents se multiplient et la société commence à remettre en question le manque de sécurité. Les industries concernées s'opposent souvent avec véhémence à l'imposition de normes de sécurité contraignantes avec les arguments suivants:

- Le produit est réputé sûr, les accidents sont le fait des utilisateurs.
- Les normes de sécurité ne sont pas considérées comme étant nécessaires, elles ruinent le secteur au niveau économique.
- Les normes de sécurité empêchent l'innovation.

Le livre de Ralph Nader de 1965, «Unsafe at any Speed», illustre ces tensions. La publication du livre a entraîné, après concertation avec l'industrie automobile, l'introduction des ceintures de sécurité, des crash tests ainsi que du rappel de séries entières de produits[16]. À ses débuts, l'industrie de l'aviation a elle-même lutté contre les essais des moteurs d'avions. Lorsqu'ils ont tout de même été introduits, plus de la moitié des moteurs ont échoué aux tests[17].

[16] Unsafe at Any Speed: The Designed-In Dangers of The American Automobile
https://en.wikipedia.org/wiki/Unsafe_at_Any_Speed
[17] A History of Aviation Safety: Featuring the U.S. Airline System
https://www.amazon.com/History-Aviation-Safety-Featuring-Airline/dp/144900797X

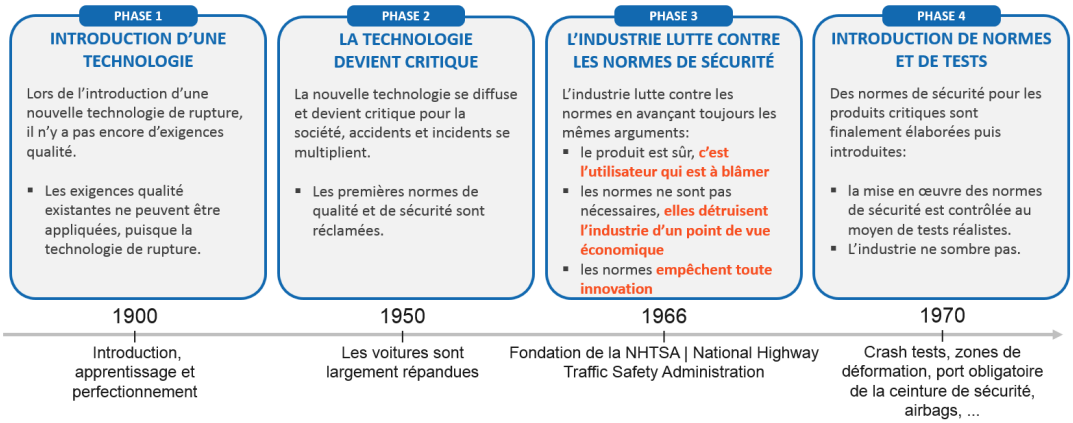


Illustration 4: Les industries de l'automobile et de l'aviation ont d'abord lutté contre l'introduction de normes de qualité. L'absence de ces normes et tests ne serait plus concevable aujourd'hui.

À l'heure actuelle, le manque de normes de sécurité et de tests dans ces industries serait inconcevable. Aussi bien l'industrie de l'automobile que celle de l'aviation sont toujours considérées comme des innovateurs de premier plan.

Dans tous les secteurs critiques de l'industrie, les contrôles qualité par des organismes indépendants font partie de la procédure d'homologation des produits, comme dans l'industrie automobile, l'aviation, la technique médicale, l'énergie, l'industrie agro-alimentaire, etc. Le secteur des TIC est le seul à ne disposer de quasiment aucune norme contraignante qui garantisse la sécurité ou l'intégrité de ses produits. Il n'existe ainsi pas de responsabilité pour les produits logiciels et les mises à jour de sécurité doivent être considérées comme des actions de rappel de logiciels défectueux à la charge du client.

Leçons pour la société numérique

Comme expliqué ci-dessus, la société a introduit dans le cadre de toutes les technologies critiques ou présentant des dommages potentiels élevés (par ex. dans les industries de l'agro-alimentaire, pharmaceutique, des transports, de l'énergie, de la construction, etc.) des normes pour garantir la qualité et la sécurité. Celles-ci sont soutenues et contrôlées par des tests réalistes. Le manque de normes et de tests pour les produits numériques doit être considéré comme critique face à l'importance croissante de ces produits.

L'histoire de la technologie donne à penser que la société développera et mettra en place des normes de qualité contraignantes pour les produits numériques également, dont des contrôles par des procédures de test et d'analyse réalistes. L'expérience nous montre que l'introduction de normes de qualité contraignantes n'entraînera pas l'effondrement de l'industrie concernée. Un débat autour des questions suivantes et le développement des thèmes correspondants par la société, l'industrie et les responsables politiques sont inéluctables:

- Quelles sont les exigences minimales en matière d'intégrité et de sécurité des produits et services numériques?
- Quelles exigences minimales s'appliquent à quels types de produits, services, domaines d'utilisation ou secteurs industriels numériques?
- Comment contrôlons-nous le respect des exigences minimales, non seulement lors de l'autorisation, mais aussi pendant l'ensemble du cycle de vie?

Ces normes de qualité contraignantes correspondent dans l'industrie automobile aux mesures de sécurité actives et passives auxquelles nous faisons confiance telles que le verre de sécurité, les systèmes de freinage à plusieurs circuits, les airbags, les crash tests, les contrôles périodiques des véhicules à moteur, etc.

Perspectives et mesures

Pour sécuriser la chaîne d'approvisionnement, il faut en conséquence introduire des mesures à différents niveaux.

La responsabilité du fabricant et du fournisseur

Les fabricants et fournisseurs doivent pouvoir être tenus responsables de la sécurité et de la qualité des produits ou services numériques ainsi que de leur fabrication. Des contrats types spécifiques aux secteurs (Annexe sur la sécurité) qui documentent les critères de sécurité pertinents doivent être mis au point. Les questions de sécurité auront ainsi plus de poids que des accords individuels entre client et fabricant.

Les exigences minimales importantes devant figurer dans l'annexe sur la sécurité peuvent être par exemple:

- Le fabricant s'engage à une divulgation coordonnée (Coordinated Disclosure) (ISO 29147) concernant le traitement des vulnérabilités rapportées. Il documente la mise en œuvre du processus, les interlocuteurs et le délai de traitement[18].

- Le fabricant s'engage à documenter de façon exhaustive et définitive tous les «comptes par défaut» (Default Accounts), mots de passe, certificats et clés intégrés dans le produit.

- Le fabricant accorde le droit au client de contrôler l'intégrité et la sécurité du matériel et des logiciels (ingénierie inverse) sans violation des droits de propriété intellectuelle (IPR, Intellectual Property Rights).

En cas de découvertes ultérieures (par ex. vulnérabilités ou portes dérobées), le fabricant peut, en tant qu'auteur, être tenu responsable (pas de «déni plausible») et le client a la possibilité, en cas d'incidents de sécurité, d'identifier sa cause (vérification judiciaire, ingénierie inverse).

La confiance et la transparence en sont améliorées, puisque le fabricant porte sa part de responsabilité. Les comportements fautifs peuvent avoir des conséquences et, dans le pire des cas, entraîner l'exclusion du marché.

[18] ISO/IEC 29147:2014 Divulgation de vulnérabilité https://www.iso.org/fr/standard/45170.html

Exigences applicables aux produits

Des mises à jour de sécurité sont requises pendant toute la durée de vie d'un produit numérique. Beaucoup de produits numériques ont une durée de vie de plusieurs dizaines d'années (par ex. les compteurs électriques, systèmes de contrôle) et leur remplacement est difficilement envisageable ou trop onéreux (par ex. après la faillite du fabricant).

Avant la mise en place de produits critiques, au minimum une des dispositions suivantes doit être présente:

- Le code source est disponible librement (Open Source).
- Avant l'achat, le code source dans sa version la plus récente est déposé auprès d'un organisme indépendant, en cas de faillite du fabricant, le code source est communiqué au client.

En tout cas, les produits pouvant être mis en réseau concernés doivent disposer d'un mécanisme robuste et sûr afin de pouvoir y installer les mises à jour de sécurité rapidement et de façon souple. On garantit ainsi la possibilité de protéger des produits critiques pendant toute leur durée de vie, y compris après la disparition du fabricant.

Laboratoire de cybertests indépendant

La société connectée doit être en mesure d'analyser et d'évaluer l'intégrité et la sécurité des produits numériques par le biais de tests indépendants et crédibles.

Ces tests doivent comprendre au minimum les points suivants:

- Une analyse du code source (dans la mesure où il est disponible), de la configuration et des paramétrages.
- L'analyse des logiciels et du matériel par ingénierie inverse si nécessaire.
- L'évaluation des risques révélés par les résultats, la coordination de la communication avec le mandant et le fabricant (divulgation coordonnée).
- La publication des résultats.

L'organisation des compétences correspondantes nécessite du temps et un laboratoire de test avec un équipement de pointe ainsi que des spécialistes qualifiés et des contacts étroits avec l'industrie, les milieux académiques et la communauté de la sécurité. Un échange international est nécessaire à long terme.

Vision pour une Suisse digitale

La capacité à contrôler de façon indépendante et efficace les produits numériques, y compris l'ingénierie inverse de puces et de firmware, gagnera en importance dans un futur proche. Par le passage croissant au numérique des fonctions quotidiennes et critiques, le besoin de cette capacité va croître dans l'industrie, tout comme dans les administrations, la police et l'armée. On peut s'attendre à ce que les cybertests deviennent bientôt des missions centrales et nationales.

La capacité de mener des tests efficaces sur les logiciels et le matériel informatique doit être considérée comme une compétence essentielle de la société numérique.

Pour ne pas être exclusivement dépendante de partenaires externes pour cette compétence essentielle à l'avenir, la Suisse doit établir rapidement, sur le modèle du laboratoire de chimie de Spiez[19], un laboratoire de cybertests en partenariat avec l'industrie, les milieux académiques et les autorités. Le laboratoire de cybertests servira à la réalisation et à la coordination des tests pour le compte de l'industrie, du pays ou d'organisations internationales.

En tant que nation neutre disposant d'une jurisprudence stable et d'une longue tradition comme siège d'institutions internationales, la Suisse est prédestinée à devenir un centre de compétences et à exploiter un laboratoire de cybertests indépendant.

[19] Laboratoire Spiez https://www.labor-spiez.ch/fr/lab/ubu/index.htm

Conclusion

De par l'utilisation hâtive ainsi que l'approvisionnement et la diffusion en partie non contrôlés de produits numériques, la société numérique court actuellement le risque de développer des problèmes de sécurité qui ne se manifesteront qu'à long terme et ne pourront être corrigés qu'avec des investissements considérables.

- Le manque de normes de qualité et de sécurité ainsi que de tests correspondants pour les produits numériques doivent, face à leur importance croissante, être considérés comme critiques.

- Sans contrôle qualité fiable des produits numériques, nous devons partir du principe que des composants compromis sont déjà en service aujourd'hui. La sécurité des produits numériques doit être vérifiée grâce à des tests crédibles et indépendants.

- Pour ne pas être exclusivement dépendante de partenaires externes en matière de cybertests, la Suisse devrait établir sans délai, sur le modèle du laboratoire de chimie de Spiez, un laboratoire de cybertests en partenariat avec l'industrie, les milieux académiques et les pouvoirs publics.

- Des exigences minimales contraignantes pour la sécurité des produits numériques doivent être élaborées en collaboration avec les partenaires (industrie, milieux académiques, pouvoirs publics).

- Dans ce cadre, la cybersécurité ne peut pas se limiter aux logiciels, à la sécurité réseau et aux facteurs humains. L'intégrité et la sécurité du matériel doivent aussi être prises en compte.

La capacité de réaliser des tests efficaces sur les logiciels et le matériel informatique doit être considérée comme une compétence essentielle de la société numérique. La société numérique se doit de s'attaquer au thème de la sécurité de la chaîne d'approvisionnement et de créer les conditions requises (ressources, cadre juridique, formation, etc.) afin d'empêcher les défauts connus et évitables. Ce n'est qu'en procédant ainsi que les opportunités offertes par le passage au numérique surpasseront ses risques dans le futur.