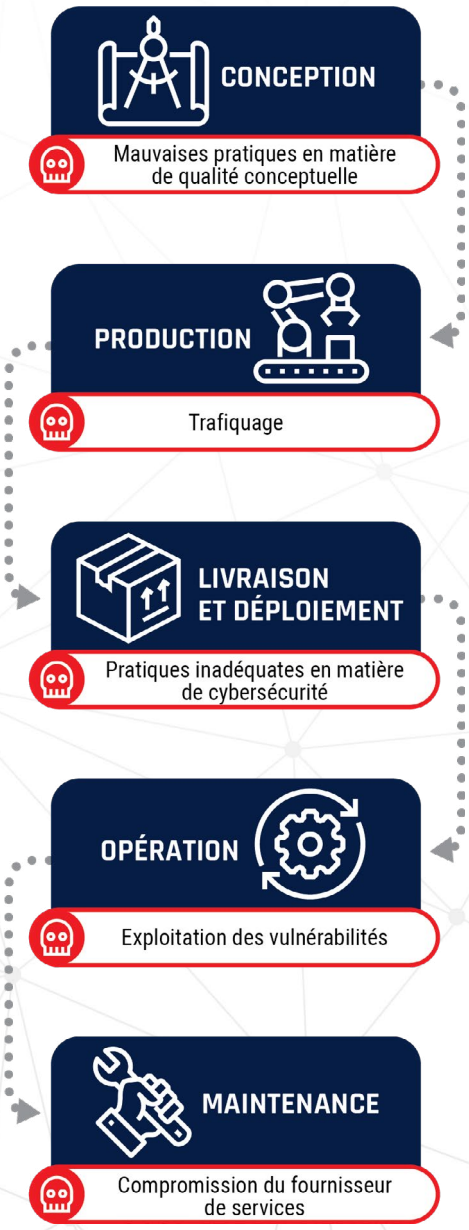
MENACES À LA CHAÎNE D'APPROVISIONNEMENT ET ESPIONNAGE INDUSTRIEL

Par chaîne d'approvisionnement, on entend le processus nécessaire à la conception, la fabrication et la distribution d'équipement et de produits, ce qui comprend le matériel informatique et les logiciels. Les étapes de ce processus complexe sont souvent confiées à des entités différentes.

Processus de la chaîne d'approvisionnement



Le niveau de sécurité de la chaîne d'approvisionnement est déterminé par son maillon le plus faible. Toute compromission de la sécurité d'une chaîne d'approvisionnement pourrait permettre à un auteur de cybermenace d'exploiter un dispositif, ou l'un de ses composants, dès sa connexion au réseau sécurisé d'une entreprise. Les chaînes d'approvisionnement peuvent être compromises avant ou après la livraison d'un produit ou service, ou au cours des mises à jour logicielles et des mises à niveau matérielles.

« Chaque maillon d'une chaîne d'approvisionnement mondiale peut présenter un risque pour la cybersécurité. »

Les auteurs de menaces peuvent également tirer parti des relations de confiance entre les entreprises. Par exemple, la mise en commun des données et des réseaux essentiels de plusieurs entreprises, entrepreneurs ou partenaires commerciaux fournit aux auteurs de cybermenaces l'occasion d'accéder à ces réseaux partagés et de les exploiter en vue d'atteindre la cible voulue. La compromission de nombreux dispositifs peut aider à dissimuler la motivation, l'identité et la cible prévue de l'auteur de menace.

Les auteurs de cybermenaces parrainés par des États cherchant à stimuler la croissance de leurs secteurs des technologies et de la défense pratiquent également le cyberespionnage industriel partout dans le monde, y compris au Canada. Le risque est encore plus grand pour les entreprises canadiennes qui font des affaires à l'étranger.

QUE FAIT LE GOUVERNEMENT DU CANADA?

Le Centre canadien pour la cybersécurité travaille en étroite collaboration avec des intervenants des secteurs essentiels afin de formuler des conseils et de l'orientation qui aideront à atténuer les risques liés à la chaîne d'approvisionnement dans les infrastructures essentielles dont les Canadiens dépendent au quotidien.

Par exemple, le Programme d'examen de la sécurité, mis en place par le Centre de la sécurité des télécommunications en 2013, a permis d'atténuer les menaces contre les technologies 3G, 4G et LTE au sein de la chaîne d'approvisionnement du secteur des télécommunications. Jusqu'à présent, le CST et ses partenaires gouvernementaux ont collaboré avec des entreprises représentant plus de 99 % du marché de la téléphonie mobile au Canada en vue d'atténuer le risque de cyberespionnage et de perturbation des réseaux. Ce programme a permis de limiter les risques en excluant certaines pièces d'équipement et certains services des zones sensibles des réseaux de télécommunications du Canada.

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ | ÉVALUATION DES CYBERMENACES NATIONALES 2018

CONSEILS PRATIQUES POUR LES PROPRIÉTAIRES ET EXPLOITANTS D'ENTREPRISES

- Poser des questions aux partenaires, aux fournisseurs et autres fournisseurs de services concernant leurs pratiques de sécurité.
- Procéder à l'évaluation des risques liés aux fournisseurs, partenaires et autres fournisseurs de services.
- Protéger l'information au niveau organisationnel. Il est possible de renforcer la sécurité en accordant aux fournisseurs concernés un accès limité à l'information ou au réseau.
- Intégrer, surveiller et défendre les passerelles Internet.
- Appliquer des correctifs aux applications et aux systèmes d'exploitation.
- Fournir aux employés des programmes de formation et de sensibilisation sur mesure.
- Pour en savoir plus, prière de visiter cyber.gc.ca