LA SÉCURITÉ DES DISPOSITIFS. PRÉVENIR LES CYBERATTAQUES

Valeria CUCOARĂ

Departement Inginerie Logiciel et Automatique, groupe FI-231, Faculté d'Ordinateurs, Informatique et Microelectronique, Université Technique de Moldavie,Chișinău, Moldova

Auteur correspondant, Cucoară Valeria, valeria.cucoara@isa.utm.md

Coordinateur scientifique **Daniela ISTRATI**, lect. univ., daniela.istrati@ia.utm.md

Sommaire. *Actuellement, la protection des données dans l'Internet des Objets est essentielle pour garantir la sécurité des informations échangées et stockées au sein de l'écosystème interconnecté des appareils. Généralement, les facteurs critiques incluent une authentification robuste des appareils, le cryptage des données, la gestion sécurisée des accès, et des mises à jour logicielles régulières pour corriger les vulnérabilités. En outre, renforcer la sensibilisation des utilisateurs et promouvoir les normes de sécurité sont indispensables pour assurer un environnement IoT sûr et inspirer confiance à l'ère d'une société numérique interconnectée. Cependant, les cyberattaques sont courantes et représentent un sujet d'intérêt populaire, en particulier lorsqu'elles sont rapportées par les médias. De plus, il convient de souligner que la plupart de ces cyberattaques ont touché des milliers, voire des millions de personnes dans le monde. Il s'agit notamment de cyberattaques contre des plateformes de réseaux sociaux, des sites web hébergeant des données personnelles et d'autres.*

Mots clés: *confidentialité, intégrité, authentification, surveillance, risqués*

Introduction

Les environnements virtuels créés par les cyberinfrastructures sont actuellement omniprésents dans notre vie quotidienne, tant sur le plan personnel que professionnel. Cependant, l'émergence des nouvelles technologies nous expose à des risques accrus qui peuvent gravement nuire aux individus et aux organisations. Malheureusement, la question de la cybersécurité est souvent négligée [1].

Il est essentiel que les organisations reconnaissent les risques liés à l'utilisation des technologies et à la gestion des données et qu'elles réagissent de manière proactive en sensibilisant leurs employés. Comprendre les différentes menaces et vulnérabilités associées à l'environnement numérique est essentiel pour mettre en place des contrôles efficaces.

La mise en œuvre de contrôles internes visant à sécuriser de manière adéquate les actifs informationnels d'une organisation nécessite une planification minutieuse et une définition claire des objectifs. Toutefois, pour être efficaces, ces contrôles doivent impliquer l'ensemble du personnel, et pas seulement les spécialistes des technologies de l'information.

Il est important de souligner que la sécurité de l'information ne peut être garantie par les seules mesures techniques. Un personnel qualifié et formé joue un rôle crucial dans ce processus. En effet, la plupart des incidents de sécurité sont souvent le résultat d'une mauvaise gestion et organisation et, dans une moindre mesure, de faiblesses dans les mécanismes de sécurité.

Le fonctionnement et les perspectives d'évolution de la cybersécurité

La cybersécurité fonctionne en combinant plusieurs mesures de protection pour empêcher la perturbation des processus, l'accès non autorisé aux informations, leur modification, leur destruction ou leur utilisation abusive. Ces mesures comprennent l'utilisation de pare-feu, de logiciels antivirus, de systèmes de détection des attaques, le cryptage des données, des politiques de sécurité strictes et des formations régulières pour sensibiliser les employés aux bonnes pratiques en matière de sécurité informatique [2].

En plus, la cybersécurité implique une surveillance constante de l'environnement numérique afin de détecter les nouvelles menaces et d'y répondre dès qu'elles apparaissent. Il peut s'agir d'analyser les journaux d'activité, de contrôler le trafic réseau, d'utiliser des technologies d'intelligence artificielle pour détecter les comportements suspects et de collaborer avec d'autres organisations et experts en sécurité pour partager des informations sur les menaces.

Actuellement, il n'existe pas de solution unique de cybersécurité pour les entreprises. Au lieu de cela, diverses mesures de protection sont combinées pour prévenir la perturbation des processus et de l'accès aux informations, leur modification, leur destruction ou leur conservation en vue d'obtenir un résultat. Cette protection doit évoluer en permanence pour contrer de manière proactive les nouvelles cybermenaces [3].

Tous les aspects de la cybersécurité sont en constante évolution. Avec l'introduction de nouvelles technologies, de nouvelles vulnérabilités apparaissent. Les cybercriminels continuent d'innover dans leurs méthodes d'attaque, ce qui entraîne des conséquences de plus en plus graves.

Les avancées telles que l'intelligence artificielle et les réseaux 5G peuvent être à la fois une bénédiction pour la cybersécurité, car elles offrent des opportunités aux experts en sécurité tout en fournissant de nouvelles avenues aux cybercriminels. Bien que les menaces futures soient difficiles à prévoir, il est clair que la cybersécurité doit adopter une approche proactive pour faire face à l'évolution constante des menaces.

État actuel des cyberattaques : complexité croissante et impact sur la société

Les cyberattaques représentent des actions frauduleuses effectuées par des cybercriminels pour compromettre des systèmes informatiques, des réseaux et des appareils électroniques dans le but d'obtenir des avantages financiers, des informations sensibles ou de causer des dommages à des organisations et à des particuliers. Ces attaques peuvent prendre diverses formes, du phishing (méthode de cyberfraude par laquelle les criminels tentent d'obtenir des informations sensibles) [4] aux logiciels malveillants, en passant par l'exploitation des failles de sécurité et les attaques par déni de service distribué (DDoS) [5].

Ces dernières années ont vu une augmentation significative de la complexité et de la fréquence des cyberattaques. En outre, les technologies émergentes telles que l'intelligence artificielle et l'internet des objets ont ouvert aux cybercriminels de nouvelles possibilités de commettre des attaques de manière innovante.

Les statistiques montrent que le nombre et l'impact des cyberattaques ont considérablement augmenté ces dernières années, entraînant des pertes financières considérables et portant atteinte à la réputation et à la confiance des organisations touchées. L'évolution rapide des technologies et la dépendance croissante à un environnement numérique ont fait des cyberattaques une menace de plus en plus grande pour la société [6].

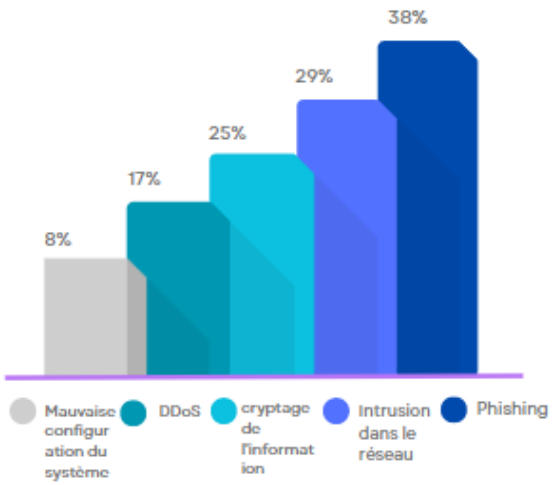

Figure 1. Statistiques sur les cyberattaques pour l'année 2023

Pour faire face à cette évolution des cyberattaques, il est essentiel d'adopter une approche proactive et globale de la cybersécurité. Cela inclut la mise en œuvre de solutions de sécurité avancées, la mise à jour régulière des systèmes et des logiciels, la formation et la sensibilisation continues des employés, ainsi que la surveillance constante de l'activité du réseau et des utilisateurs afin de détecter les menaces et d'y répondre rapidement.

Aussi, la coopération entre les organisations et les gouvernements est cruciale dans la lutte contre les cyberattaques. Le partage d'informations sur les menaces et les vulnérabilités peut contribuer à renforcer la sécurité et à réduire l'impact des cyberattaques sur la société dans son ensemble [7].

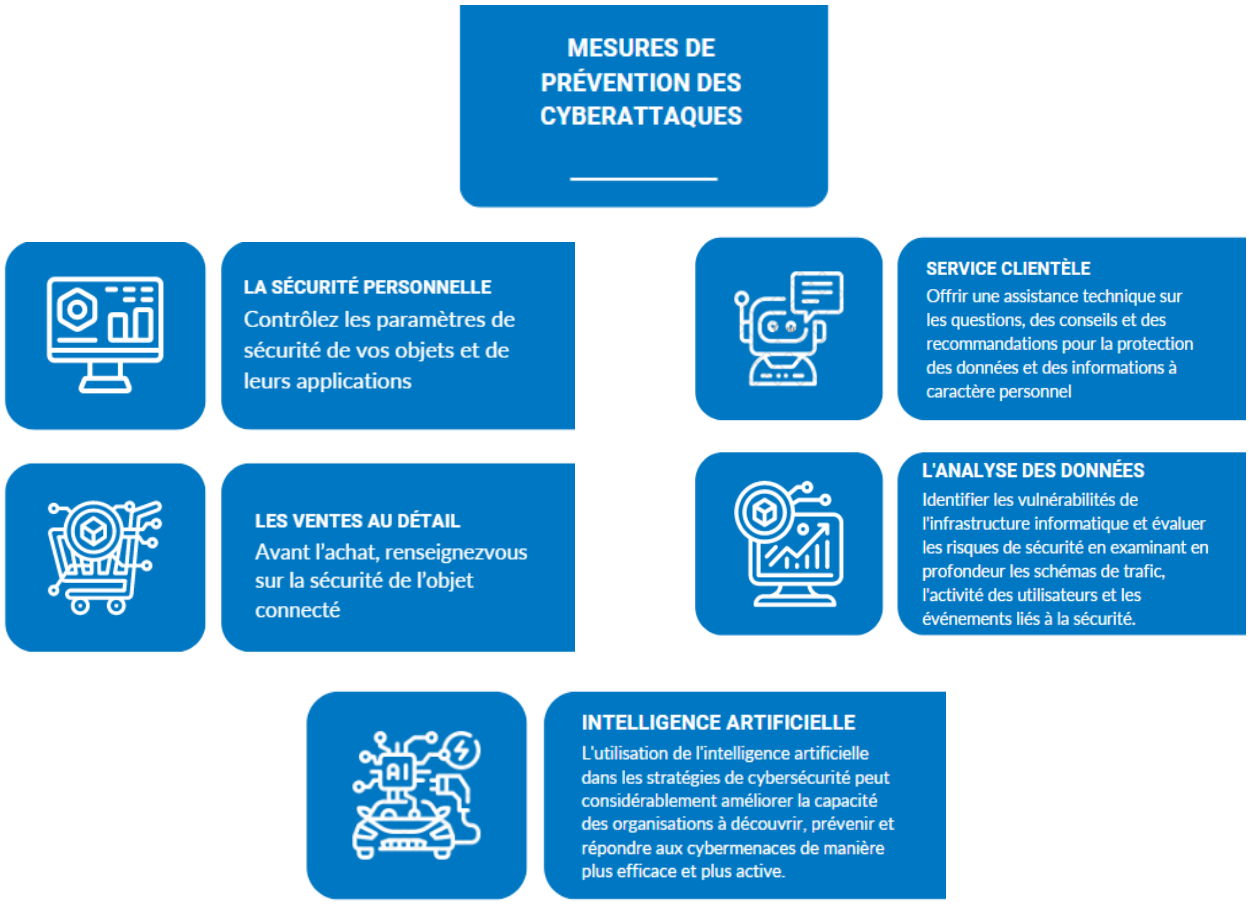

Figure 2. Mesures de prévention des cyberattaques

Conclusions

La cybersécurité est essentielle à l'ère numérique pour protéger les informations confidentielles se protéger contre les cybermenaces, préserver la confiance, respecter les réglementations et garantir la résilience et la continuité des opérations en ligne. Il s'agit d'un processus continu qui nécessite une surveillance permanente, des mises à jour régulières et des initiatives proactives afin de rester en avance sur les nouvelles menaces cybernétiques émergentes.

Les cyberattaques constituent une menace croissante et sérieuse pour les systèmes informatiques, les réseaux et les personnes. Avec l'évolution rapide des technologies et l'apparition de nouveaux moyens pour les cybercriminels de compromettre les systèmes, il est devenu important que les organisations et les individus adoptent des mesures proactives pour se protéger contre ces attaques.

Les références

[1] Securite cibernitique,Moldavie,2018 https://stisc.gov.md
[2] Auteur: Ioan-Cosmin Mihai, Costel Ciuchi, Gabriel Petrică (coord.)Considérations sur les défis et les orientations futures en matière de cybersécurité Editura Sitech,Roumanie, 2019
[3] Auteur: Ioan-Cosmin Mihai, Gabriel Petrică Sécurité de l'information. 2e édition, révisée et complétée Maison d'édition Sitech,Roumanie,2014
[4] *Sécurité informatique – Ethical Hacking : Apprendre l'attaque pour mieux se défendre,France,2017*
[5] Auteurs: Gildas Avoine (Auteur), Pascal Junod (Auteur) *Cybersécurité et hygiène numérique au quotidien* 129 bonnes pratiques à adopter pour se protéger,France, 2024
[6] Auteur: Anouch Seydtaghia Comment se protejer des cyberattaques, https://www.letemps.ch/articles?query=PME%3A+comment+se+prot%C3%A9ger+des+cyberattaques%3F&button=
[7] Auteur: Jean-Luc Raymond ,Protection contre les risques https://www.francenum.gouv.fr/guides-et-conseils/protection-contre-les-risques/professionnels-de-sante-comment-prevenir-les