LA CYBER-SÉCURITÉ

Valeria GURANDA[1*]

[1]*Université Technique de Moldavie, Faculté Ordinateurs, Informatique et Microélectronique, Département Génie Logiciel el Automatique, Groupe FI-191, Chişinău, République de Moldavie*

*Autorul corespondent: Valeria Guranda, valeria.guranda@isa.utm.md

Résumé. *Il n'existe pas de définition standard et universellement acceptée de la cybersécurité. D'une manière générale, ce concept couvre toutes les garanties et mesures prises pour protéger les systèmes informatiques et leurs utilisateurs contre les accès non autorisés, les attaques et les dommages, afin de garantir la confidentialité, l'intégrité et la sécurité.*

Mots clés *: cybersécurité, concept, système, informatiques, confidentialité.*

Introduction

L'environnement virtuel, généré par le cyber infrastructures, fait déjà partie intégrante de la vie personnelle et professionnelle. Cependant, les nouvelles technologies impliquent de nouveaux risques qui peuvent affecter gravement l'individu ou l'organisation, cependant la cybersécurité est bien trop rare.

Il est important que les organisations soient conscientes des risques associés à l'utilisation de la technologie et à la gestion de l'information et abordent ce problème de manière positive en sensibilisant les employés, en comprenant la typologie des menaces et des vulnérabilités propres aux environnements informatisés et en appliquant des pratiques de contrôle. Les actifs informationnels d'une institution nécessitent une planification rigoureuse et une identification précise des objectifs de cette institution. Cependant, pour être efficaces, ces contrôles doivent cibler tous les collaborateurs et pas seulement ceux de la DSI ou qui sont directement liés à ce domaine.

Les objectifs pour une bonne sécurité :

- Améliorer la confidentialité, l'intégrité et la disponibilité des données et informations diffusées dans les systèmes d'information et de communication utilisés par les fonctionnaires ;
- Fournir les moyens pour guider et soutenir l'activité liée à la sécurité de l'information au sein des institutions, en définissant des contrôles et des mesures visant à identifier et réduire les risques et vulnérabilités de sécurité qui se manifestent en leur sein [1].

Les nombreux types de cybermenaces peuvent être classés en fonction de leurs effets sur les données (divulgation, modification, destruction ou refus d'accès) ou selon les principes de base de la sécurité de l'information violés, comme le montre la figure 1 ci-dessous. L'encadré 1 décrit un certain nombre d'exemples d'attaques. À mesure que la sophistication des attaques contre les systèmes informatiques augmente, nos mécanismes de défense deviennent moins efficaces.

Figure 1. Types de menaces et principes de sécurité qu'elles posent.

Types de cyberattaques

Les types de cybermenaces les plus courants sont: [2,3]

Phishing. Le phishing est une forme de fraude dans l'environnement en ligne qui consiste à utiliser des techniques pour manipuler l'identité d'individus / organisations afin d'obtenir des avantages matériels ou des informations confidentielles. Les attaquants utilisent diverses techniques d'ingénierie sociale pour persuader les victimes de divulguer des données d'authentification. Les cibles les plus courantes sont les sites Web des institutions financières, telles que les banques.

SPAM : e-mail non sollicité, souvent commercial, publicité pour des produits et services douteux, utilisé par l'industrie du marketing et les propriétaires de sites avec un contenu indécent. Les messages de spam sont envoyés en utilisant ordinateurs infectés par des chevaux de Troie, qui font partie d'un botnet (un réseau d'ordinateurs compromis utilisé pour envoyer du spam ou des attaques sur des sites Internet à l'insu des propriétaires de ces ordinateurs).

VIRUS : Les virus informatiques sont des programmes qui se copient sur le système compromis à l'insu de l'utilisateur. Le virus infectera ainsi des composants du système d'exploitation ou d'autres programmes informatiques.

TROYEN : ces programmes se présentent sous la forme de programmes légitimes, qui sont effectivement créés dans le but de voler des données confidentielles, ou pour permettre aux utilisateurs ou programmes accès non autorisé au système infecté.

ROOTKIT : Un rootkit est un ensemble d'utilitaires conçus pour maintenir le contrôle ou l'accès à un ordinateur. Après l'installation, le rootkit utilise les fonctions du système d'exploitation pour «se cacher » afin qu'il ne soit pas détecté.

HACKER : une personne qui entre dans les ordinateurs (sans le consentement du propriétaire), généralement en accédant aux contrôles administratifs.

Règles d'utilisation acceptables

Pour garantir l'intégrité de l'ordinateur et de vos données personnelles, je vous recommande de suivre ces règles :

- Éviter autant que possible d'utiliser le compte d'administrateur du système d'exploitation. Il est nécessaire de créer un compte utilisateur ne disposant pas de tous les privilèges propres au compte administrateur.

- Utiliser des mots de passe complexes. En règle générale, tous les mots de passe associés à tout compte d'utilisateur doivent comporter au moins 10 caractères et être complexes, au sens où ils incluent des caractères spéciaux, des chiffres, des lettres minuscules et majuscules ;
- Ignorer des appels téléphoniques, des visites ou des courriels non sollicités de personnes demandant des informations personnelles [4].

Figure 2. Intégrité d'ordinateur

La navigation sur l'internet sécurisée

Les navigateurs sont des programmes utilisés pour naviguer sur Internet. Ils permettent d'accéder et de visualiser des sites, de parcourir des liens, de télécharger des fichiers depuis Internet, etc. pour réduire les risques [4].

Concernant la navigation sur Internet, les recommandations suivantes doivent être suivies :

- Éviter d'accéder aux liens marqués comme dangereux par la solution de sécurité installée sur le système ou par le navigateur Internet.
- Désactiver l'exécution de script dans les navigateurs.
- Utiliser un antivirus.
- Ne jamais enregistrer les mots de passe de votre compte dans les navigateurs Web.

Bibliographie :

1. Ioan-Cosmin Mihai, Costel Ciuchi, Gabriel Petrică: *Considerations on Challenges and Future Directions in Cybersecurity.*
2. Ioan-Cosmin Mihai: *Procedures for Detecting Cybercrime Activities on Websites.*
3. Challenges to effective EU cybersecurity policy, [online]. 2019, [accédé le 19.02.2021]. Disponible: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_RO.pdf
4. What is Cyber Security ? [online]. 2018, [accédé le 19.02.2021]. Disponible : https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security