**A C A D E M I A  R O M Â N Ă**
SECȚIA DE ȘTIINȚE ECONOMICE, JURIDICE ȘI SOCIOLOGIE
INSTITUTUL NAȚIONAL DE CERCETĂRI ECONOMICE ”COSTIN C. KIRIȚESCU”

# DIGITALIZARE ȘI SECURITATE CIBERNETICĂ ÎN CONTEXTUL COVID-19

**Coordonator**
Meghișan-Toma Georgeta-Mădălina, CS III, Dr.

București
mai 2020

## *Introducere*

Cercetările în domeniul securității cibernetice subliniază faptul că 75% din companii se confruntă, în medie, cu un atac cibernetic pe an (https://comunic.ro/specialistii-in-securitate-cibernetica-sunt-prea-increzatori-in-eficacitatea-instrumentelor-de-securitate-75-dintre-companii-sunt-atacate-cel-putin-o-data-pe-an/, accesat 05.05.2020) Mai mult, 32% din organizații experimentează un atac cibernetic drept consecință a faptului că un angajat lucrează în exteriorul perimetrului de securitate al companiei. (Chapman, 2020) În anul 2019, 50% din angajați au lucrat de acasă, în medie 2,5 zile pe săptămână. (Murphy, 2019) În contextul actual al pandemiei generate de COVID-19, procentul angajaților care lucrează de acasă, 5 zile pe săptămână, a ajuns la aproape 100%. (https://comunic.ro/lucrul-de-la-distanta-vine-si-cu-amenintari-de-securitate-cibernetica/, accesat 25.04.2020)

## *Metodologia de cercetare*

În lucrarea de față, analiza asupra măsurilor de securitate cibernetică implementate de companii, se realizează la nivelul statelor membre ale Uniunii Europene pentru anul 2019, pentru a avea un punct de plecare în realizarea de comparații față de perioada actuală 2020, în contextul pandemiei COVID-19. Setul de variabile a fost ales, luând în considerare disponibilitatea datelor în cadrul bazei de date EUROSTAT. (Tabelul 1)

**Tabelul 1 Variabile pentru măsuri de securitate cibernetică utlizate de către companii**

| Variabile |
|---|
| (Item 1) Autentificarea printr-o parolă puternică |
| (Item 2) Actualizarea la zi a sistemului de software (inclusiv a sistemului de operare) |
| (Item 3) Identificarea și autentificarea utilizatorului prin metode biometrice, implementate de către întreprindere |
| (Item 4) Tehnici de criptare pentru date, documente și e-mailuri |
| (Item 5) Backup de date într-o locație separată (inclusiv copie de rezervă în cloud) |
| (Item 6) Controlul accesului la rețea (gestionarea accesului dispozitivelor și a utilizatorilor la rețeaua întreprinderii) |
| (Item 7) VPN (Rețeaua virtuală privată extinde o rețea privată de-a lungul unei rețele publice pentru a asigura schimbul de date în cadrul rețelei publice) |
| (Item 8) Păstrarea fișierelor de conectare pentru analiză, după incidente de securitate |
| (Item 9) Evaluarea riscului în domeniul TIC, de exemplu, prin evaluarea periodică a probabilității și a consecinței incidentelor de securitate în cadrul TIC |
| (Item 10) Teste de securitate în cadrul TIC |

Sursa: Prelucrarea proprie a autorului

Pentru analiza principalelor măsuri de securitate în domeniul TIC, folosite de companiile din statele membre ale Uniunii Europene, a fost utilizată analiza factorială. Testul KMO și Bartlett are o valoare acceptabilă (0,783).

Variabilele cu o calitate a reprezentării peste 0,5, reținute în analiza finală, sunt:

- (Item 1) Autentificarea printr-o parolă puternică (0,539);
- (Item 2) Actualizarea la zi a sistemului de software (inclusiv a sistemului de operare) (0,776);
- (Item 4) Tehnici de criptare pentru date, documente și e-mailuri (0,551);
- (Item 5) Backup de date într-o locație separată (inclusiv copie de rezervă în cloud) (0,789);
- (Item 6) Controlul accesului la rețea (gestionarea accesului dispozitivelor și a utilizatorilor la rețeaua întreprinderii) (0,679);
- (Item 7) VPN (Rețeaua virtuală privată extinde o rețea privată de-a lungul unei rețele publice pentru a asigura schimbul de date în cadrul rețelei publice) (0,837);
- (Item 8) Păstrarea fișierelor de conectare pentru analiză după incidente de securitate (0,821);
- (Item 9) Evaluarea riscului în domeniul TIC, de exemplu, prin evaluarea periodică a probabilității și a consecinței incidentelor de securitate în cadrul TIC (0,777)
- (Item 10) Teste de securitate în cadrul TIC (0,779).

O singură dimensiune permite explicarea fenomenului în proporție de 72,746% prin cele 9 variabile.

Coeficientul Alpha Cronbach are valoarea 0,951, ceea ce permite afirmația că scala are o viabilitate acceptabilă a coerenței interne.

Matricea corelației subliniază corelații între toți cei 9 itemi, ceeea ce întărește concluzia că cele 9 variabile măsoară același fenomen (măsuri de securitate în domeniul TIC, luate de către întreprinderile din cadrul statelor membre ale Uniunii Europene). (Tabelul 2)

**Tabelul 2 Corelații între variabilele analizate**

| | | Item 1 | Item 2 | Item 4 | Item 5 | Item 6 | Item 7 | Item 8 | Item 9 | Item 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| Spearman's rho | Item 1 | 1,000 | 0,707** | 0,476* | 0,439* | 0,532** | 0,410* | 0,415* | 0,710** | 0,586** |
| | Item 2 | | 1,000 | 0,629** | 0,794** | 0,645** | 0,752** | 0,785** | 0,818** | 0,753** |
| | Item 4 | | | 1,000 | 0,665** | 0,439* | 0,615** | 0,703** | 0,549** | 0,554** |
| | Item 5 | | | | 1,000 | 0,565** | 0,820** | 0,795** | 0,714** | 0,704** |
| | Item 6 | | | | | 1,000 | 0,704** | 0,670** | 0,603** | 0,584** |
| | Item 7 | | | | | | 1,000 | 0,865** | 0,741** | 0,772** |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Item 8 | | | | | | | 1,000 | 0,764** | 0,806** |
| | Item 9 | | | | | | | | 1,000 | 0,958** |
| | Item 10 | | | | | | | | | 1,000 |

Sursa: Prelucrarea proprie a autorului, utilizând software de analiză statistică SPSS 21.00 pentru Windows

## *Rezultate*

Din analiza realizată, rezultă că întreprinderile care utilizează TIC au nevoie de implementarea unor măsuri de securitate în acest domeniu. Potrivit rezultatelor cercetării, principalele măsuri de securitate utilizate de întreprinderile din statele membre ale Uniunii Europene, la nivelul anului 2019, sunt (Tebelul 3):

- (Item 1) Autentificarea printr-o parolă puternică (cu variații între 53% și 91%);
- (Item 2) Actualizarea la zi a sistemului de software (inclusiv a sistemului de operare) (cu variații între 61% și 95%);
- (Item 4) Tehnici de criptare pentru date, documente și e-mailuri (cu variații între 19% și 59%);
- (Item 5) Backup de date într-o locație separată (inclusiv copie de rezervă în cloud) (cu variații între 40% și 89%);
- (Item 6) Controlul accesului la rețea (gestionarea accesului dispozitivelor și a utilizatorilor la rețeaua întreprinderii) (cu variații între 38% și 85%);
- (Item 7) VPN (Rețeaua virtuală privată extinde o rețea privată de-a lungul unei rețele publice pentru a asigura schimbul de date în cadrul rețelei publice) (cu variații între 15% și 62%);
- (Item 8) Păstrarea fișierelor de conectare pentru analiză după incidente de securitate (cu variații între 17% și 64%);
- (Item 9) Evaluarea riscului în domeniul TIC, de exemplu, prin evaluarea periodică a probabilității și a consecinței incidentelor de securitate în cadrul TIC (cu variații între 14% și 60%)
- (Item 10) Teste de securitate în cadrul TIC (cu variații între 15% și 52%).

**Tablelul 3 Statistică descriptivă asupra variabilelor analizate**

| | N | Minim | Maxim | Medie | Std. Deviation |
|---|---|---|---|---|---|
| Item 1 | 28 | 53,00 | 91,00 | 74,1429 | 10,34485 |
| Item 2 | 28 | 61,00 | 95,00 | 83,3929 | 8,40784 |
| Item 4 | 28 | 19,00 | 59,00 | 36,7857 | 10,41138 |
| Item 5 | 28 | 40,00 | 89,00 | 72,4286 | 12,60343 |
| Item 6 | 28 | 38,00 | 85,00 | 62,2857 | 10,21929 |
| Item 7 | 28 | 15,00 | 62,00 | 40,1429 | 12,31294 |
| Item 8 | 28 | 17,00 | 64,00 | 42,1071 | 12,95959 |
| Item 9 | 28 | 14,00 | 60,00 | 33,8929 | 11,97633 |
| Item 10 | 28 | 15,00 | 52,00 | 35,6071 | 9,77275 |
| Valid N (listwise) | 28 | | | | |

Sursa: Prelucrarea proprie a autorului, utilizând software de analiză statistică SPSS 21.00 pentru Windows

În contextul pandemiei generate de COVID-19, angajații au fost nevoiți să se adapteze unei noi realități- munca de la distanță, cu toate riscurile implicate: conectarea la rețele publice și la rețele Wi-Fi, ransomeware, infecții malware, spinonaj corporativ, phishing, dispozitive personale cu software depășit, descentralizarea controlului IT, dificultăți în securizarea dispozitivelor contectate la Internet. (https://comunic.ro/lucrul-de-la-distanta-vine-si-cu-amenintari-de-securitate-cibernetica/, accesat 25.04.2020)

## *Concluzii*

Din analiza realizată, rezultă că la nivelul anului 2019, companiile din statele membre ale Uniunii Europene au implementat măsuri de securitate în domeniul TIC, dar acestea nu acoperă în totalitate nevoile de securitate în contextul actual al pandemiei generate de coronavirus.

Drept urmare, propunerile care se adaugă la ceea ce companiile au implementat deja în domeniul securității TIC, în contextul COVID-19, vizează (https://comunic.ro/microsoft-anunta-noi-capabilitati-in-ai-si-automatizare-pentru-securitate-cibernetica/, accesat 15.04.2020; https://comunic.ro/lucrul-de-la-distanta-vine-si-cu-amenintari-de-securitate-cibernetica/, accesat 25.04.2020; https://comunic.ro/specialistii-in-securitate-cibernetica-sunt-prea-increzatori-in-eficacitatea-instrumentelor-de-securitate-75-dintre-companii-sunt-atacate-cel-putin-o-data-pe-an/, accesat 09.05.2020; ):

- **Identificarea și autentificarea utilizatorului prin metode biometrice, implementate de către întreprindere;**
- **Instruirea de bază a angajaților în domeniul securității cibernetice;**
- **Implementarea unei soluții antivirus fiabile, adaptabilă pentru toate dispozitivele de conectare;**
- **Activarea firewall la nivelul browser-ului de căutare utilizat;**
- **Activarea opiunilor antifurt a dispozitivelor de conectare: localizarea dispozitivului; Touch ID; Face ID etc. ;**
- **Utilizarea inteligenței artificiale (AI) și a automatizării pentru creșterea gradului de securitate cibernetică;**
- **Utilizarea multi-cloud de către companii pentru salvarea datelor;**
- **Creșterea gradului de gestionare și a riscurilor interne de securitate cibernetică;**
- **Testarea instrumentelor de securitate de către companii la intervale de timp mult mai mici (cel puțin o dată pe lună);**
- **Crearea unei proceduri de răspuns la un atac cibernetic din partea angajaților companiei;**

Noua realitate la care companiile trebuie să se adapteze vizează desfășurarea activităților remunerate de acasă și după starea de urgență, cum este cazul angajaților din marile corporații- de exemplu, Facebook (peste 48.000 de angajați), Google (peste 120.000 de angajați) etc. (https://comunic.ro/news/angajatii-google-si-facebook-ar-putea-lucra-de-acasa-pana-la-final-de-an/, accesat 09.05.2020) Astfel, se poate explica gradul ridicat de importanță pe care companiile trebuie să îl acorde domeniului securității cibernetice, pentru buna desfășurare a activității angajaților lor. (https://comunic.ro/accenture-achizitioneaza-divizia-de-securitate-cibernetica-symantec-de-la-broadcom/, accesat 05.05.2020)

## Bibliografie


1. Chapman, P. (2020). Are your IT staff ready for the pandemic-driven insider threat?, Network Security, issue 4, volume 2020, pp. 8-11;
2. Murphy, H. (2019). How remote working increase cyber security risks", Financial Times, 8 Dec 2019, https://www.ft.com/content/f7127666-0c80-11ea-8fb7-8fcec0c3b0f9, accesat 09.05.2020;

3. https://comunic.ro/specialistii-in-securitate-cibernetica-sunt-prea-increzatori-in-eficacitatea-instrumentelor-de-securitate-75-dintre-companii-sunt-atacate-cel-putin-o-data-pe-an/, accesat 05.05.2020;
4. https://comunic.ro/lucrul-de-la-distanta-vine-si-cu-amenintari-de-securitate-cibernetica/, accesat 25.04.2020;
5. https://comunic.ro/microsoft-anunta-noi-capabilitati-in-ai-si-automatizare-pentru-securitate-cibernetica/, accesat 15.04.2020;
6. https://comunic.ro/news/angajatii-google-si-facebook-ar-putea-lucra-de-acasa-pana-la-final-de-an/, accesat 09.05.2020;
7. https://comunic.ro/accenture-achizitioneaza-divizia-de-securitate-cibernetica-symantec-de-la-broadcom/, accesat 05.05.2020.