CASE- Centrul pentru Cercetare Socială și Economică

Cartografierea amenințărilor cibernetice pentru IMM-urile din Uniunea Europeană

Rezumat

Strategia Comisiei Europene pentru IMM-uri, care urmărește Europă durabilă și digitală, a recunoscut vulnerabilitatea IMM-urilor față de amenințările cibernetice și a identificat securitatea cibernetică drept unul dintre aspectele cheie ale perfecționării digitale. Și la nivel global, amenințările cibernetice apar printre principalele riscuri globale pe termen scurt (World Economic Forum, 2021) și devin o amenințare constantă pentru majoritatea întreprinderilor pe fondul transformării digitale accelerate indusă de criza Covid-19 (OECD, 2021).

Acest raport identifică incidentele apărute pe internet, inclusiv phishingul, malware-ul și atacurile pe web, ca fiind **cele mai frecvente** amenințări cibernetice relevante pentru IMM-urile din UE. În conformitate cu ENISA (2020), alte amenințări cibernetice importante includ, de asemenea, spam-ul, refuzul de serviciu, furtul de identitate, încălcările de date, amenințările din interior, rețelele bot, manipularea fizică și daunele, scurgerile de informații, spionajul cibernetic și criptojacking-ul. În același timp, în timp ce accesul la internet și trecerea la munca de la distanță ar putea crește expunerea IMM-urilor la riscurile de securitate cibernetică, factorul uman este o altă sursă importantă de vulnerabilitate digitală, deoarece aproximativ 84% din toate atacurile cibernetice din UE se bazează pe ingineria socială pentru a atrage oamenii să divulge informații sensibile sau să acceseze link-uri care pot conține fișiere rău intenționate (ENISA, 2020).

Analizele fiecărei țări prezentate în acest raport subliniază în continuare importanța tot mai mare a discuțiilor privind securitatea cibernetică la nivel național și confirmă gradul relativ scăzut de cunoștințe privind securitatea cibernetică în rândul IMM-urilor. Conform rezultatelor Eurobarometrului 2020, ponderea respondenților care au declarat că nu sunt „bine informați" cu privire la riscurile criminalității cibernetice a fost de 67% pentru România și Italia, 55% pentru Spania și 43% pentru Polonia. Mai mult, la nivelul companiei, doar 7% dintre IMM-urile din România și-au făcut angajații conștienți de obligațiile lor în materie de securitate TIC prin instruiri obligatorii. La rândul lor, IMM-urile din Spania, Polonia și Italia au evoluat peste media UE, cu cifre de 20%, 30% și, respectiv, 34%. Cu toate acestea, atunci când s-a luat în considerare diferența dintre IMM-uri și întreprinderile mari, România și Italia au una dintre cele mai mici lacune la nivelul UE - doar 21 pp și respectiv 23 pp. În timp ce Spania are un decalaj relativ mai mare, cu 27%, a reușit să rămână sub media pp-30 UE-27 și diferența de 35 pp înregistrată în Polonia.

Astfel, IMM-urile UE rămân deseori în urma întreprinderilor mari în ceea ce privește conștientizarea și pregătirea de a face față amenințărilor cibernetice proliferante. Mai important, amenințările cibernetice mai mari și mai frecvente sunt, de asemenea, cele în privința cărora nivelul de conștientizare din UE rămâne cel mai scăzut. Lipsa de conștientizare și de angajament din partea conducerii, în special, este provocarea comună și cel mai des citată (ENISA, 2021). În consecință, doar 30% din IMM-urile din UE recurg la mai mult decât măsurile de bază decât securitatea cibernetică și mai puțin de 30% din IMM-urile din UE-27 își conștientizează angajații cu privire la obligațiile lor de securitate TIC prin cursuri de formare obligatorie - aproape de două ori mai puțin comparativ cu o întreprindere mare.

With the support of the Erasmus+ programme of the European Union. This document and its contents reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Co-funded by the Erasmus+ Programme of the European Union

Alte **provocări structurale** care subminează o mai mare pregătire a IMM-urilor includ, de asemenea, o conștientizare scăzută a personalului în materie de securitate cibernetică, protecție inadecvată a informațiilor critice și sensibile, lipsa bugetului, lipsa unor specialiști dedicați IT și de securitate cibernetică și lipsa unor orientări adecvate privind securitatea cibernetică specifică IMM-urilor.

O serie de inițiative la nivelul UE, incluzând, printre altele, Strategia UE de securitate cibernetică, Agenția UE pentru securitate cibernetică, precum și cadrele SMESEC și Make_SME_Digital, permit reducerea lacunelor de competențe și consolidarea rezilienței colective împotriva amenințărilor cibernetice. Acestea sunt susținute în continuare de inițiativele la nivel de țară - de exemplu, Platforma națională poloneză pentru securitate cibernetică și PWCyber Cybersecurity - Program de cooperare și Cadrul național italian pentru securitate cibernetică și Consorțiul național interuniversitar pentru tehnologia informației (CINI) - care stabilesc cadre naționale de securitate cibernetică și susțin digital dezvoltarea abilităților la nivel local.

Cu toate acestea, așa cum s-a discutat în acest raport și în profilurile de țară individuale, sunt necesare acțiuni politice mai cuprinzătoare pentru a combate lipsa sistemică a capacităților de securitate cibernetică în rândul IMM-urilor din UE. Acestea ar trebui să se concentreze pe consolidarea:

(i) **conștientizarea cibernetică** în rândul IMM-urilor prin promovarea unei mai bune înțelegeri a securității cibernetice în general și adaptarea conținutului și canalelor campaniilor de informare în funcție de contextul și nevoile sectoriale ale IMM-urilor.

(ii) **reziliența cibernetică** a IMM-urilor prin crearea de standarde și ghiduri privind securitatea cibernetică, axate pe IMM-uri, precum și prin promovarea utilizării cadrelor de gestionare a riscurilor cibernetice în cadrul IMM-urilor și facilitarea accesului la securitatea cibernetică.

(iii) **receptivitatea cibernetică** a IMM-urilor prin promovarea instruirilor voluntare și obligatorii în rândul angajaților și sprijinirea dezvoltării unor protocoale de securitate simplificate.

With the support of the Erasmus+ programme of the European Union. This document and its contents reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Co-funded by the Erasmus+ Programme of the European Union