CASE- Centrum Analiz Społeczno-Ekonomicznych

Mapowanie zagrożeń cybernetycznych dla mikro-, małych i średnich przedsiębiorstw w UE

Streszczenie

W strategii Komisji Europejskiej dotyczącej MŚP na rzecz zrównoważonej i cyfrowej Europy uznano podatność MŚP na zagrożenia cybernetyczne i określono bezpieczeństwo cybernetyczne jako jeden z kluczowych aspektów podnoszenia kwalifikacji w zakresie technologii cyfrowych. Również na poziomie globalnym cyberzagrożenia pojawiają się wśród głównych krótkoterminowych zagrożeń globalnych (Światowe Forum Ekonomiczne, 2021) i stają się stałym zagrożeniem dla większości przedsiębiorstw w obliczu przyspieszonej transformacji cyfrowej wywołanej kryzysem Covid-19 (OECD, 2021).

W niniejszym sprawozdaniu określono incydenty internetowe, w tym phishing, złośliwe oprogramowanie i ataki internetowe, jako najczęstsze cyberzagrożenia istotne dla unijnych MŚP. Zgodnie z ENISA (2020), inne ważne cyberzagrożenia obejmują również spam, odmowę usługi, kradzież tożsamości, naruszenia danych, zagrożenia wewnętrzne, botnety, fizyczne manipulacje i szkody, wyciek informacji, cyberszpiegostwo i cryptojacking. Jednocześnie, podczas gdy dostęp do Internetu i praca zdalna mogą zwiększać narażenie MŚP na ryzyko związane z bezpieczeństwem cybernetycznym, czynnik ludzki jest kolejnym ważnym źródłem podatności na zagrożenia cyfrowe, jako że około 84% wszystkich ataków cybernetycznych w UE opiera się na socjotechnice w celu nakłonienia ludzi do ujawnienia poufnych informacji lub kliknięcia na link, który może zawierać złośliwe pliki (ENISA, 2020).

Analizy krajowe przedstawione w niniejszym raporcie podkreślają rosnące znaczenie tematyki cyberbezpieczeństwa na poziomie krajowym i potwierdzają stosunkowo niski poziom wiedzy na temat cyberbezpieczeństwa wśród małych i średnich przedsiębiorstw. Zgodnie z wynikami Eurobarometru 2020, odsetek respondentów, którzy stwierdzili, że nie są "dobrze poinformowani" o zagrożeniach związanych z cyberprzestępczością wyniósł 67% w Rumunii i we Włoszech, 55% w Hiszpanii i 43% w Polsce. Ponadto, na poziomie przedsiębiorstwa, tylko 7% MŚP w Rumunii uświadomiło swoim pracownikom ich obowiązki w zakresie bezpieczeństwa TIK poprzez obowiązkowe szkolenia. Z kolei MŚP w Hiszpanii, Polsce i Włoszech osiągnęły wyniki zbliżone do średniej unijnej, a nawet ją przewyższające, odpowiednio 20%, 30% i 34%. Jeśli jednak wziąć pod uwagę różnice pomiędzy MŚP a dużymi przedsiębiorstwami, Rumunia i Włochy mają jedne z najmniejszych różnic w całej UE - odpowiednio tylko 21 i 23 punkty procentowe. Podczas gdy Hiszpania ma relatywnie wyższą lukę na poziomie 27%, udało jej się pozostać poniżej średniej dla UE-27 wynoszącej 30 punktów procentowych oraz luki 35 punktów procentowych odnotowanej w Polsce.

W związku z tym unijne MŚP często pozostają w tyle za dużymi przedsiębiorstwami pod względem świadomości i gotowości do radzenia sobie z rozprzestrzeniającymi się cyberzagrożeniami. Co ważniejsze, największe i najczęstsze cyberzagrożenia są również tymi, na temat których poziom świadomości w UE jest najniższy. Powszechnym i najczęściej wymienianym wyzwaniem jest w szczególności brak świadomości i zaangażowania ze strony kierownictwa (ENISA, 2021). W rezultacie tylko 30 proc. unijnych MŚP stosuje więcej niż podstawowe środki bezpieczeństwa cybernetycznego, a mniej niż 30 proc. MŚP w UE-27 uświadamia swoich pracowników o ich obowiązkach w zakresie

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

bezpieczeństwa TIK poprzez obowiązkowe szkolenia - prawie dwukrotnie mniej niż w przypadku dużych przedsiębiorstw.

Inne wyzwania strukturalne, które osłabiają większą gotowość MŚP, obejmują również niską świadomość pracowników w zakresie bezpieczeństwa cybernetycznego, nieodpowiednią ochronę krytycznych i wrażliwych informacji, brak budżetu, brak dedykowanych specjalistów IT i specjalistów ds. bezpieczeństwa cybernetycznego oraz brak odpowiednich wytycznych w zakresie bezpieczeństwa cybernetycznego specyficznych dla MŚP.

Szereg inicjatyw na poziomie UE, w tym m.in. Strategia Bezpieczeństwa Cybernetycznego UE, Agencja Bezpieczeństwa Cybernetycznego UE, a także ramy MŚP i Make_SME_Digital, pozwalają na zniwelowanie różnic w umiejętnościach i wzmocnienie zbiorowej odporności na cyberzagrożenia. Są one dodatkowo wspierane przez inicjatywy na poziomie krajowym - np. polską Krajową Platformę Bezpieczeństwa Cybernetycznego i Program Współpracy w Dziedzinie Bezpieczeństwa Cybernetycznego PWCyber oraz włoskie Krajowe Ramy Bezpieczeństwa Cybernetycznego i Krajowe Konsorcjum Międzyuniwersyteckie na rzecz Technologii Informacyjnych (CINI) - które ustanawiają krajowe ramy bezpieczeństwa cybernetycznego i wspierają rozwój umiejętności cyfrowych na poziomie lokalnym.

Jednak, jak stwierdzono w niniejszym raporcie i w profilach poszczególnych krajów, konieczne jest podjęcie bardziej kompleksowych działań politycznych w celu rozwiązania problemu systemowego braku zdolności w zakresie bezpieczeństwa cybernetycznego wśród unijnych MŚP. Działania te powinny koncentrować się na wzmocnieniu:

(i) **świadomości cybernetycznej** wśród MŚP poprzez promowanie lepszego zrozumienia bezpieczeństwa cybernetycznego w ogóle oraz dostosowanie treści i kanałów kampanii informacyjnych do kontekstu i potrzeb sektorowych MŚP.

(ii) **odporności cybernetycznej** MŚP poprzez stworzenie norm i wytycznych w zakresie bezpieczeństwa cybernetycznego ukierunkowanych na MŚP, promowanie stosowania ram zarządzania ryzykiem cybernetycznym w MŚP oraz zwiększenie dostępności bezpieczeństwa cybernetycznego.

(iii) **reaktywności cybernetycznej** MŚP poprzez promowanie dobrowolnych i obowiązkowych szkoleń wśród pracowników oraz wspieranie rozwoju uproszczonych protokołów bezpieczeństwa.

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