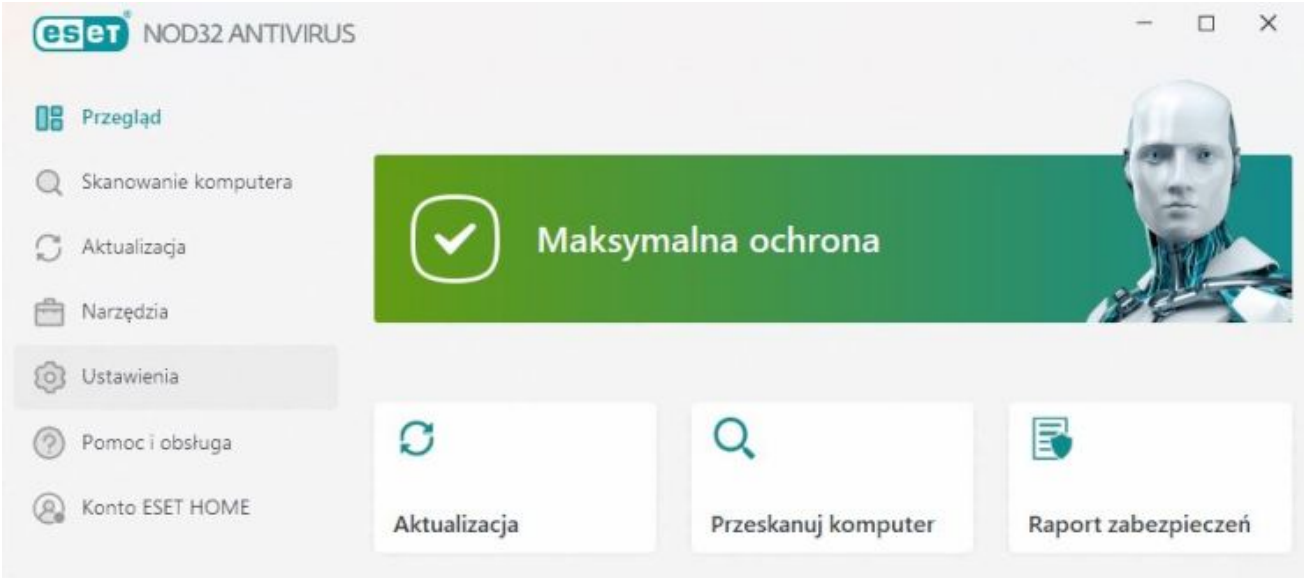
Jak wynika z najnowszego raportu ESET na temat bezpieczeństwa cyfrowego małych i średnich firm, ponad dwie trzecie z 1200 ankietowanych podmiotów (w tym 59 proc. polskich) doświadczyło w ciągu ostatnich 12 miesięcy incydentu związanego z bezpieczeństwem IT. Jego średni szacunkowy koszt wyniósł niemal 220 tys. euro, czyli ponad 1 mln złotych.



Uczestnicy badania Digital Security Sentiment, zorganizowanego przez ESET wśród europejskich i północnoamerykańskich przedsiębiorstw, wskazali także największe ich zdaniem zagrożenia w perspektywie kolejnego roku.

Według przedstawicieli polskich przedsiębiorstw jest to głównie brak świadomości cyberzagrożeń wśród pracowników, a obawy dotyczą także m.in. ograniczeń budżetowych.

Konsekwencje ataków i poczucie bezpieczeństwa

Według uczestników badania, największą biznesową konsekwencją cyberataku były: utrata danych oraz finansowe następstwa działań przestępców, co 67 proc. ankietowanych wskazało jako jedną z top 3 opcji [uczestnicy badania wskazywali opcje 1-szego, 2-go i 3-go wyboru]. Obawa o utratę zaufania partnerów biznesowych (59 proc.) znalazła się na trzecim miejscu cyber-lęków. Decydenci są zaniepokojeni możliwymi skutkami ataków, a jednocześnie
aż 70 proc. firm przyznało, że ich inwestycje w cyberbezpieczeństwo nie nadążają za zmianami w modelach funkcjonowania firm, takich jak na przykład powszechność pracy zdalnej czy hybrydowej.

> *– Sfera cyberzagrożeń nieustannie ewoluuje, a przestępcy działają wedle coraz to nowych scenariuszy, nawiązujących do zmian w rzeczywistości społecznej. Tym samym nie jest zaskoczeniem, że wobec świadomości niedostosowania własnych możliwości do realnych potrzeb, ocena potencjału MŚP co do własnej cyberodporności w perspektywie kolejnych 12 miesięcy pozostaje niska. Niespełna połowa respondentów (48 proc.) określa poziom bezpieczeństwa swoich firm jako umiarkowany lub dobry. Jako bardzo dobre ocenia go jedynie 12 proc. polskich uczestników badania – komentuje Kamil Sadkowski, starszy specjalista ds. cyberbezpieczeństwa w ESET.*

Główne ryzyka

Małe i średnie przedsiębiorstwa jako główny czynnik zwiększający ryzyko cyberataków (84%) zidentyfikowały brak świadomości cybernetycznej wśród swoich pracowników, wskazało tak przy tym 94 proc. polskich MŚP uczestniczących w badaniu, co było

największym odsetkiem wśród ankietowanych. W tym kontekście wskazywano także luki w ekosystemie partnera/dostawcy (79%) oraz ataki prowadzone na zlecenie państw w kontekście konfliktu rosyjsko-ukraińskiego (78%).

> *– Można na te wyniki spojrzeć z pewną dozą optymizmu. Mimo globalnych wydarzeń będących niewątpliwie czynnikami wpływającymi na bezpieczeństwo IT, takich jak wojna w Ukrainie czy zmiany naszej rzeczywistości związane z następstwami pandemii COVID-19, uczestnicy badania są świadomi, że niezależnie od geopolitycznych zjawisk najsłabszym ogniwem systemu bezpieczeństwa pozostaje człowiek – ocenia Kamil Sadkowski.*

Wyzwania w obszarze cyberbezpieczeństwa

Najnowsze dane z raportu ESET Threat Report (opublikowany we wrześniu br.) pokazują 20 proc. wzrost liczby wykrytych zagrożeń w sferze bezpieczeństwa IT od początku 2022 roku, w porównaniu do analogicznego okresu roku ubiegłego. Aż 83 proc. firm ankietowanych w najnowszym raporcie Digital Security Sentiment, ESET ocenia, że „cyberwojna jest bardzo realnym zagrożeniem, które może dotknąć każdego”, co sugeruje, że stale rosnące zagrożenia znacząco wpływają na nastroje wśród przedstawicieli MŚP. Ponadto 74 proc. małych i średnich firm w Europie i Ameryce Północnej uważa, że są bardziej podatne na cyberataki niż duże przedsiębiorstwa.

Respondenci jako główne zagrożenia cyberbezpieczeństwa na najbliższe 12 miesięcy

wskazali:

- Złośliwe oprogramowanie (łącznie 70 proc.)
- Ataki na strony internetowe (łącznie 67 proc.)
- Ransomware (łącznie 65 proc.)
- Problemy bezpieczeństwa stron trzecich (64 proc.)
- Ataki typu „DDoS” (60 proc.)
- Ataki typu Remote Desktop Protocol (łącznie 60 proc.)

Wśród polskich uczestników badania ESET jako najważniejsze wyzwania w obszarze cyberbezpieczeństwa ponad połowa wskazała na ograniczenia budżetowe ograniczające możliwość inwestycji i fałszywe alerty (po 52 proc.),
a także obawę o dotrzymanie kroku rozwojowi technologii w tym obszarze (47 proc.).

###

W raporcie ESET Digital Security Sentiment poświęconemu tematyce bezpieczeństwa cyfrowego małych i średnich firm z 2022 r., przebadano ponad 1200 decydentów zajmujących się tematyką cyberbezpieczeństwa w tym segmencie przedsiębiorstw w Europie i Ameryce Północnej. Raport analizuje nastroje w szerszym kontekście ostatnich wydarzeń na świecie kształtujących postrzeganie bezpieczeństwa przez MŚP. Uczestnicy badania wskazywali opcje 1-szego, 2-go i 3-go wyboru, co do kwestii, o które byli pytani.

źródło informacji: dagma.com.pl