Łukasz Masztalerz,
Aplikant Adwokacki, DGTL Kibil Piecuch i Wspólnicy S.K.A.

Phishing wall
- jak zbudować ludzką zaporę przeciwko cyberatakom?

O cyberzagrożeniach łatwo mówić, gdy doszło już do incydentu bezpieczeństwa. Wówczas dowiadujemy się, że firma musiała zapłacić okup za uzyskanie klucza do zaszyfrowanych przez złośliwe oprogramowanie danych. Biznes na chwilę obniża poziom ciśnienia krwi, a cyberprzestępca liczy wpływy. Jak wynika z rynku zachodniego i badań zajmującej się cyberbezbieczeństwem firmy Infrascale: już 78% małych i średnich przedsiębiorców działających w modelu B2B zapłaciło pierwsze okupy w wyniku cyber ataku[1].

Co więcej, większość z przedsiębiorców, która nie padła jeszcze ofiarą ataku w badaniach odpowiada, że w razie ataku zapłaciłaby okup: po pierwsze dlatego, by szybko uzyskać odzyskać pliki, a po drugie, by ochronić renomę firmy.

Nieco rzadziej zdarza się, że ofiara ataku nie tylko nie chce płacić okupu, ale i uzyskuje skuteczną pomoc. Tak było w 2019 r. w przypadku gminy Kościerzyna[2]. Gmina ta po ataku zgłosiła się z prośbą o pomoc do CSIRT NASK. Sprawą zainteresował się także ekspert jednego z dostawców oprogramowania antywirusowego, który napisał skuteczny dekryptor.

Tym razem zaatakowany miał nieco więcej szczęścia. Wydaje się jednak, że na co dzień mógłby oddychać o wiele spokojniej. Jest to możliwe, jeśli organizacja stale wspiera rozwój cyberświadomości wśród jej pracowników oraz przygotowuje procedury, a tym samym zespół na krytyczny moment.

Do oczywistego znaczenia budowania cyber świadomości w ramach dobrych praktyk biznesowych przekonywać nie zamierzam. Warto jednak podkreślić, że nie są to zagadnienia już zupełnie abstrakcyjne i wprowadzone w celu wyróżnienia się na tle konkurencji lub zadbania o interes użytkownika.

> (...) większość z przedsiębiorców, która nie padła jeszcze ofiarą ataku w badaniach odpowiada, że w razie ataku zapłaciłaby okup

Już obecnie są to także obowiązki regulacyjne, które z jednej strony generują po stronie przedsiębiorców dodatkowy wysiłek w zakresie budowania zgodności (compliance), a z drugiej strony zapewniają bezpieczeństwo rynku, jego indywidualnych użytkowników, a niekiedy służą ochronie bezpieczeństwa narodowego.

Aktywność regulatorów, poczynając od poziomu europejskiego (dyrektywa NIS i projektowana NIS II) i kończąc na krajowym porządku jako wykonawcy porządku europejskiego sprowadza się do ustalania reguł dla sektorów krytycznych z punktu widzenia bezpieczeństwa rynku wspólnotowego. Kolejno, naturalnym wyzwaniem dla regulacji na poziomie wspólnotowym okazuje się ich jednakowa lub mieszcząca się w granicach dyrektywy implementacja do porządków krajowych. Okazuje się, że newralgicznymi zagadnieniami, są tutaj, m. in.:

[1] wyznaczenie podmiotów objętych regulacją, [2] jednakowe mechanizmy motywowania podmiotów obowiązanych do przestrzegania nowych norm, czy [3] ujednolicony system certyfikacji.

Można ten wątek kontynuować banalnym stwierdzeniem, że jeśli nie przyznamy organowi nadzoru „superkompetencji", to system na poziomie europejskim nie będzie skuteczny. I jest to wątek, który widać w zapatrywaniach organów europejskich w takich obszarach prawa, jak przeciwdziałanie praniu pieniędzy (AML), czy ochrona danych osobowych (RODO). Ten temat widoczny jest także w obszarze cyberbezpieczeństwa, gdzie uchwalenie NIS 2 uzasadnia się, m. in. potrzebą jednolitego systemu podmiotów obowiązanych, czy zgodnym systemem certyfikacji.

W przepisach europejskich na nowo definiuje się obecnie podmioty kluczowe (essential). Zawarto w nich naturalnie sektor transportowy, finansowy, zdrowotny, czy **energetyczny**, a także uwzględniono wśród nich dostawców usług chmurowych. Niejednokrotnie normy w zakresie cyberbezpieczeństwa kreują obowiązki dla podmiotów z takich sektorów gospodarki, które już wcześniej objęte były nadzorem z uwagi na bezpieczeństwo uczestników rynku lub interes fiskalny państwa. W związku z tym zwracać należy uwagę na sektorowe stanowiska organów nadzoru, które bezpośrednio i niekiedy bardziej szczegółowo poruszają kwestie z obszaru cyberbezpieczeństwa.

I tak będzie, m. in. w przypadku komunikatu Urzędu Komisji Nadzorowanego w sprawie przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej. W komunikacie tym Urząd wprost wskazuje, że za obsługę usług związanych z chmurą powinni odpowiadać pracownicy, których kompetencje


fot. Bermix Studio on Unsplash

w tym zakresie potwierdzone zostały odpowiednią dokumentacją szkoleniową lub imiennymi zaświadczeniami w zakresie odpowiednim do używania tego typu usług.

Podobnie wypowiada się Europejski Urząd Nadzoru Bankowego w zakresie zarządzania technologiami ICT, który stoi na stanowisku, że instytucje finansowe powinny opracować program szkoleniowy, a w tym okresowe programy zwiększenia świadomości na temat bezpieczeństwa przeznaczone dla wszystkich pracowników instytucji. Celem takiej rekomendacji ma być budowa odpowiednich kompetencji w zespołach danej instytucji, ale i ograniczeniu błędów ludzkich, kradzieży, oszustw, czy innych nadużyć.

To wszystko pozwala stwierdzić, że istota doskonalenia pracowników i organizacji w zakresie cyber-świadomości odzwierciedlona została już na poziomie formalnym. Wyzwaniem wydaje się być zastosowanie w praktyce tego, co przyjął papier.

W ramach najbliższego webinarium „Nowej Energii" razem z Państwem będziemy poszukiwać odpowiedzi na pytanie o rolę edukacji członków załogi w budowie systemu cyberbezpieczeństwa. Odpowiemy również na pytanie: czy świadomość w zakresie cyberzagrożeń oraz stały proces szkolenia to tylko dobre praktyki, czy także obowiązki prawne?

Rejestracja na webinarium: www.nowa-energia.com.pl □

Przypisy

1 Infrascale.com, dostęp z dnia 17.11.2021 r. https://www.infrascale.com/press-release/infrascale-survey-reveals-close-to-half-of-smbs-have-been-ransomware-attack-targets/

2 Sekurak.pl, dostęp z dnia 17.11.2021 r. https://sekurak.pl/gmina-koscierzyna-skutecznie-odszyfrowala-swoje-dane-po-ataku-ransomware/