**Jak bezpiecznie przeprowadzić transformację cyfrową firmy?**

* **8 na 10 polskich przedsiębiorstw jest w trakcie transformacji cyfrowej.**
* **Stałym elementem zmian IT firmy powinny być audyty bezpieczeństwa.**
* **Testować należy nie tylko rozwiązania techniczne, ale też reakcje pracowników.**

Cyfryzacja jest przyszłością firm. To fakt, z którym nikt się nie spiera, co widać w „twardych” liczbach. Jak wynika z tegorocznego raportu „BARIERY i TRENDY. Transformacja technologiczna firm w Polsce”, aż 78% średnich i dużych przedsiębiorstw w Polsce jest w trakcie transformacji cyfrowej. Co chcą osiągnąć? Dążą przede wszystkim do zwiększenia swojej efektywności, poprzez poprawienie funkcjonowania kluczowych procesów, wzrostu sprzedaży oraz optymalizacji kosztów. To wszystko jednak wymaga czasu i pieniędzy – z czego zresztą zdają sobie sprawę zarządzający firmami (80% uczestników badania wskazała te czynniki jako główne wyzwania).

– *Dlatego równolegle ze zmianą poszczególnych procesów produkcyjnych, sprzedażowych czy organizacyjnych, należy też zweryfikować politykę bezpieczeństwa firmy. Zwłaszcza w obszarze cyber, żeby wszystkich tych wysiłków nie przyćmił skuteczny atak hakerski. W końcu cyfryzacja firmy nieodłącznie wiąże się z uruchamianiem nowych systemów informatycznych oraz zwiększeniem liczby urządzeń połączonych ze sobą sieciowo. To dodatkowe furtki dla cyberprzestępców i trzeba się dobrze przygotować na wzrost ryzyka cyberataku* – mówi Michał Bukontt, Dyrektor Sprzedaży w Sprint S.A.

Rosnące ryzyko potwierdzają obserwacje ekspertów od cyberbezpieczeństwa – wraz ze wzrostem wykorzystania w biznesie urządzeń z obszaru tzw. Internetu Rzeczy, w skrócie IoT (wyróżniana jest nawet odrębna kategoria urządzeń – Industrial IoT), zwiększa się liczba ataków hakerskich na te sprzęty. Już dwa lata temu firma F-secure zauważyła 3-krotny wzrost liczby ataków na te urządzenia. Co więcej, hakerzy tworzą nawet specjalne malware, przeznaczone do atakowania właśnie IoT czy IIot – np. „Mirai” czy „Katana”.

**Jak przeprowadzić audyt bezpieczeństwa w firmie?**

Sprawdzenie firmowej infrastruktury IT na wypadek ataków cybernetycznych powinno składać się z kilku różnych etapów. Przede wszystkim należy przeprowadzić zarówno testy zewnętrzne, jak i wewnętrzne. Te pierwsze mają za zadanie zobaczyć czy możliwe jest nieautoryzowane uzyskanie dostępu do firmowych danych lub systemów za pośrednictwem sieci zewnętrznej. Najczęściej poprzez symulowanie ataku na sieć bezprzewodową przedsiębiorstwa za pośrednictwem Internetu. Drugie, wewnętrzne polegają na sprawdzeniu słabych punktów i nieprawidłowości w konfiguracji urządzeń działających w ramach firmowej sieci wewnętrznej – to szczególną uwagę należy poświęcić wspomnianym wyżej IoT. Prowadząc te testy, należy jednak sprawdzać nie tylko aspekty techniczne, ale też weryfikować zachowania pracowników – skrupulatność w stosowaniu zasad bezpieczeństwa, podatność na błędy oraz sposoby reakcji w razie zagrożenia. To absolutne minimum.

– *Tego typu testy powinna prowadzić każda firma, niezależnie od wielkości i skali działania. Proszę pamiętać, że teraz praktycznie każdy przedsiębiorca jest podłączony w ten czy inny sposób do Internetu, więc może stać się celem hakerów. A ci nie są wybredni i najczęściej idą na „ilość”, a nie na „jakość” ofiar, ponieważ to może im się bardziej opłacić. Prowadząc masowe ataki malware czy ransomware liczą na efekt skali, zatem nawet najmniejsi przedsiębiorcy są także potencjalnym celem* – dodaje Michał Bukontt ze Sprint SA.

Ponadto, wiele firm korzysta z różnego rodzaju aplikacji webowych, jak sklepy internetowe, porównywarki i inne aplikacje osadzone na stronach internetowych. One też są coraz częściej przedmiotem ataków, więc warto przeprowadzić również testy penetracyjne skupione na ich działaniu. Szczególnie pod kątem ataków DDoS czy z wykorzystaniem technik SQL Injection. Podobnie należy postąpić w przypadku aplikacji mobilnych, jeśli firma je posiada.

**Kluczowe elementy IT, które warto zmodernizować**

Bardzo często zwiększenie zabezpieczeń sieciowych wiąże się również z koniecznością wymiany lub ulepszenia pewnych elementów infrastruktury informatycznej. Szczególną uwagę należy poświęcić samej sieci (z jakiego jej rodzaju korzystamy), jakości urządzeń zapewniających dostęp do Internetu oraz kluczowemu oprogramowaniu. Oto kilka pytań, na które warto w związku z tym odpowiedzieć:

* Czy wystarczy zwykły WLAN, czy może lepiej uruchomić WAN, może warto też korzystać z VPN?
* Czy nie należy wymienić routerów na wyższy standard WiFi?
* Czy istnieje konieczność uruchomienia dodatkowych zabezpieczeń typu WAF (zapora dla aplikacji webowych) lub rozwiązań z obszaru zabezpieczenia punktów końcowych (tzw. EDR)?

– *Proszę jednak pamiętać, że najlepsze nawet oprogramowanie i najwyższej jakości oraz generacji urządzenia nie zdadzą się na nic, kiedy nie stosujemy się do podstawowych zasad bezpieczeństwa. Dlatego modernizacji zabezpieczeń i procedur, powinny towarzyszyć dodatkowe szkolenia dla pracowników. Najlepiej, jeśli przedsiębiorcy organizują je cyklicznie, ponieważ z miesiąca na miesiąc cyberprzestępcy wymyślają nowe sposoby ataku* – zauważa Michał Bukontt ze Sprint S.A.

Źródło: Sprint S.A.