Barometr cyberbezpieczeństwa

COVID-19 przyspiesza cyfryzację firm

Wprowadzenie

Marzec 2021

KPMG.pl

Wstęp

Szanowni Państwo,

Zachęcam do zapoznania się z wynikami czwartej edycji badania KPMG „Barometr Cyberbezpieczeństwa" diagnozującego bieżące trendy i podejście polskich przedsiębiorstw w zakresie ochrony przed cyberprzestępczością. W badaniu wzięło udział 100 małych, średnich i dużych polskich firm, reprezentowanych przez osoby odpowiedzialne za zapewnienie bezpieczeństwa informacji.

Tegoroczna edycja badania odbyła się w niespotykanych dotychczas okolicznościach ogólnoświatowej pandemii. Nie będzie więc zaskoczeniem, że zapytaliśmy polskie organizacje, jak COVID-19 wpłynął nie tylko na obszar cyberbezpieczeństwa, ale ściśle związaną z nim cyfryzację. Koronawirus w przypadku większości (58%) polskich firm spowodował wzrost inicjatyw związanych z cyfryzacją. 83% organizacji wdrożyło pracę zdalną – niemal w pełni w klasycznym modelu z wykorzystaniem służbowych laptopów i szyfrowanych połączeń (VPN). Jednocześnie ponad połowa polskich firm stwierdziła wzrost podatności na cyberataki w związku z wymuszonymi przez pandemię zmianami organizacji pracy. Dla 58% polskich przedsiębiorstw koronawirus spowodował wzrost ryzyka cyberataków, jednakże jedynie w przypadku 23% firm wiązało się to ze zwiększeniem budżetu na cyberbezpieczeństwo.

Tłumaczy to wzrost o 10% odsetka polskich przedsiębiorstw dotkniętych cyberatakami w porównaniu z poprzednim rokiem. Skutków cyberprzestępczości doświadczyła w 2020 roku większość (64%) polskich firm. Co więcej, w minionym roku wzrost lub znaczący wzrost liczby prób cyberataków zanotowało 19% firm w Polsce, natomiast ich spadek odnotowało tylko 2% przedsiębiorców.

Polskie przedsiębiorstwa nadal najbardziej obawiają się zorganizowanej cyberprzestępczości. Zastanawiający jest natomiast istotny spadek poczucia zagrożenia ze strony własnych pracowników względem ubiegłych lat. Biorąc pod uwagę pracę zdalną oraz wynikające z niej osłabienie relacji oraz kontroli, spodziewać się raczej można zwiększenia ryzyka związanego z nieautoryzowanymi działaniami z wnętrza organizacji.

Polacy najbardziej obawiają się złośliwego oprogramowania (malware) oraz ataków socjotechnicznych (phishing). Skutkiem przeprowadzonych za ich pomocą cyberataków może być wyciek wrażliwych danych lub zablokowanie do nich dostępu poprzez ich zaszyfrowanie a następnie żądanie okupu.

Ciekawym wynikiem badania jest kolejny raz wysoki optymizm polskich przedsiębiorstw w kwestii oceny dojrzałości wdrożonych zabezpieczeń. Z perspektywy doświadczeń KPMG z realizowanych audytów bezpieczeństwa, wydaje się, że tak wysoka samoocena, może niestety po części wynikać z wciąż niedostatecznej świadomości polskich firm w zakresie skali i złożoności dzisiejszych cyberzagrożeń. W szczególności polskie firmy wciąż nie dostrzegają istotnego ryzyka związanego z podatnościami występującymi powszechnie w aplikacjach.

Największą barierą w budowaniu bezpieczeństwa są ponownie trudności w zatrudnieniu i utrzymaniu wykwalifikowanych pracowników. Jest to zgodne z obserwowanym od kilku lat trendem, który jedynie w zeszłym roku został chwilowo zakłócony w związku z niepewnością na rynku pracy, wywołaną pandemią koronawirusa.

Pozostaje mi życzyć Państwu przyjemnej lektury oraz wielu przemyśleń i inspiracji, które przyczynią się do wzrostu bezpieczeństwa w Państwa organizacjach.

Z poważaniem,

Michał Kurek
Partner
Szef zespołu ds. cyberbezpieczeństwa
KPMG w Polsce

Aby pobrać pełen raport zaloguj się na **kpmg.pl**