**Odporność cybernetyczna kluczem do przetrwania**

Autor: Paweł Raczyński, Dyrektor Zarządzający Kyndryl Poland i Kraje Bałtyckie

W miarę rozwoju gospodarki cyfrowej wykładniczo rośnie również zagrożenie związane z przestępczością cyfrową. Eksperci CERT Polska podają w najnowszym raporcie z działalności, że w 2022 roku odnotowali w kraju ponad 34% więcej zarejestrowanych cyber incydentów[[1]](#footnote-2), niż w roku poprzednim. Atakowane były firmy z różnych sektorów gospodarki, w tym z branży energetycznej, finansowej czy handlowej, a w trójce najczęściej zgłaszanych typów incydentów znalazły się te związane z phishingiem, szkodliwym oprogramowaniem oraz przypadkami włamań do systemów IT i na konta pocztowe.

Rosnąca liczba zagrożeń bezpośrednio przekłada się na straty finansowe dla biznesu. Organizacja Cybersecurity Ventures szacuje w swoim raporcie, że szkody spowodowane cyberatakami w 2025 roku osiągną poziom 10,5 biliona dolarów rocznie[[2]](#footnote-3). Będzie to o 300% więcej, niż dekadę wcześniej. Nic dziwnego, że prawie dziewięć na dziesięciu[[3]](#footnote-4) ankietowanych przez Gartnera członków zarządu już w 2021 roku wskazywało, że ich zdaniem naruszenie bezpieczeństwa cyfrowego w firmie stanowi ryzyko przede wszystkim biznesowe, a nie technologiczne.

Jednocześnie te deklaracje i rosnąca świadomość ryzyka wciąż nie pociągają za sobą inwestycji, które skalą i zakresem dorównywałyby zagrożeniu. Agencja IDC (International Data Corporation) prognozuje, że światowe wydatki na rozwiązania i usługi podnoszące bezpieczeństwo cyfrowe firm wyniosą w 2023 roku 219 miliardów dolarów[[4]](#footnote-5), co stanowi wzrost o 12,1% w porównaniu do roku ubiegłego. Prawie połowę tego budżetu organizacje przeznaczą na oprogramowanie, w tym to z obszaru Endpoint Security (ochrona punktów końcowych), Digital Identity Trust (zaufanie do tożsamości cyfrowej) oraz analityki i reagowania na incydenty.

To zdecydowanie krok w dobrym kierunku. Ale należy przy tym pamiętać, że w dzisiejszych czasach kluczem do rozwijania bezpiecznej firmy jest koncentracja nie tylko na obronie, ale rozwijaniu odporności cybernetycznej. Chodzi o kompleksowe podejście do zabezpieczania aplikacji i systemów o znaczeniu krytycznym, oparte na filarach, takich jak przewidywanie zagrożeń (anticipate), stawianie im oporu (withstand), powrót do pełnej operacyjności po wystąpieniu incydentu (recover) oraz adaptacja i ulepszanie strategii cyberbezpieczeństwa (adapt).

Umiejętność antycypowania ryzyka jest dla rozwoju odporności cybernetycznej niezmiernie ważna, ponieważ zmienia tok myślenia najważniejszych osób w firmie z reaktywnego na proaktywny. Gdy podchodzimy do cyberataku jako zagrożenia, które na pewno się wydarzy – pytanie tylko kiedy – łatwiej jest nam zamodelować przebieg przykładowego incydentu, zidentyfikować luki w zabezpieczeniach, które doprowadziły do jego wystąpienia oraz przeanalizować plan dalszego działania uwzględniający ograniczanie wpływu ataku na organizację. Firma, która rozwija na poważnie odporność cybernetyczną działa na co dzień w stanie podwyższonej gotowości operując tak, jakby atak już nastąpił.

######

**Kyndryl**

Kyndryl (NYSE: KD) jest największym na świecie niezależnym dostawcą usług infrastruktury IT, wspierającym tysiące klientów z obszaru enterprise w ponad 60 krajach. Firma projektuje, buduje, zarządza i modernizuje złożone, krytyczne systemy informatyczne, od których świat zależy każdego dnia. Więcej informacji: www.kyndryl.com.

1. <https://cert.pl/uploads/docs/Raport_CP_2022.pdf> [↑](#footnote-ref-2)
2. <https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/> [↑](#footnote-ref-3)
3. <https://www.gartner.com/en/newsroom/press-releases/2021-11-18-gartner-survey-finds-88-percent-of-boards-of-directors-view-cybersecurity-as-a-business-risk> [↑](#footnote-ref-4)
4. <https://www.idc.com/getdoc.jsp?containerId=prUS50498423> [↑](#footnote-ref-5)