Cyberbezpieczeństwo staje się integralną częścią wszystkich procesów

Z Łukaszem Węgrzynem, partnerem w kancelarii Kochański & Partners, rozmawiamy o największych wyzwaniach związanych dziś z cyberbezpieczeństwem; europejskich regulacjach, które dotyczą tego obszaru; konieczności przygotowania się zawczasu do nieuchronnego cyberataku; działaniach w ramach MAIN Partner Community oraz o – realizowanym wspólnie z MAIN – programie „Bezpieczny Zarząd – Dyrektor IT".

Kancelaria Kochański & Partners – w ramach wielu usług pomagających przedsiębiorcom wykorzystywać najnowsze technologie – oferuje też wsparcie w uzyskaniu gotowości do realizacji obowiązków prawnych w zakresie cyberbezpieczeństwa. Jakie są więc dziś najważniejsze wyzwania związane z cybersecurity?

Na pewno w ostatnim okresie znacząco wzrosło ryzyko ataku. Kiedyś mówiło się, że cyberataki zdarzają się sporadycznie. Teraz jest to zjawisko nagminne. Powodem jest fakt, że nasze życie w coraz większym stopniu przenosi się do sieci. Jak podaje KPMG w raporcie „Barometr cyberbezpieczeństwa", wybuch pandemii COVID-19 – w opinii 55% badanych firm w Polsce – przyczynił się do wzrostu ryzyka wystąpienia cyberataków. Aż 64% organizacji odnotowało co najmniej jeden tego typu incydent w roku 2020, a 51% firm przyznało, że konieczność organizacji pracy w trybie zdalnym była wyzwaniem w kontekście zapewnienia bezpieczeństwa. Zwiększyła bowiem podatność na wystąpienie cyberataku.

Dlatego dziś nie tylko firmy komercyjne, ale i administracja – przeglądając procedury związane z cyberbezpieczeństwem – próbują dostosować się do nowych realiów. Jednocześnie poszczególne rządy, ale i Komisja Europejska przygotowują nowe akty prawne, które mają uporządkować ten świat. KE przedstawiła np. projekty dwóch aktów prawnych: dyrektywy w sprawie: środków na rzecz wysokiego, wspólnego poziomu cyberbezpieczeństwa – NIS 2 oraz odporności podmiotów krytycznych. Z kolei w Polsce przeprowadzana jest nowelizacja Ustawy o Krajowym Systemie Cyberbezpieczeństwa, a Ministerstwo Klimatu i Środowiska opublikowało rekomendacje dotyczące zarządzania infrastrukturą techniczną i relacji z dostawcami IT.

Unia Europejska chce w szczególności poukładać tematy związane z cyberbezpieczeństwem w sektorze finansowym. Temu sektorowi dedykowana jest Digital Operational Resilience Act – DORA. Rozporządzenie to usprawnia i aktualizuje istniejące przepisy dotyczące zarządzania ICT, zarządzania ryzykami oraz zgłaszania incydentów związanych z cyberbezpieczeństwem. Wprowadza też nowe regulacje w miejscu istniejących luk, w szczególności w odniesieniu do testo-

wania operacyjnej odporności cyfrowej, wymiany informacji i zarządzania ryzykiem ze strony zewnętrznych dostawców usług ICT. DORA przyznaje również odpowiednie uprawnienia organom nadzoru finansowego w zakresie kontroli zgodności z obowiązkami wynikającymi z projektowanego rozporządzenia.

Dlaczego Komisja Europejska tak wielką wagę przykłada do tematów związanych z cyberbezpieczeństwem w sektorze finansowym?

Po kryzysie tego sektora z lat 2008–2009 wszyscy regulatorzy świata doszli do wniosku, że muszą wprowadzić regulacje, które zabezpieczą nas przed kolejnym, podobnym kryzysem. Pojawiło się wiele tego typu regulacji. Ale ostatecznie okazało się, że ważne jest nie tylko bezpieczeństwo finansowe, lecz także organizacyjne i techniczne. To ostatnie uważane jest dziś wręcz za najważniejsze.

> Cyberbezpieczeństwo stało się jednym z trzech głównych priorytetów zarządów. Kierowane przez nich organizacje muszą zawczasu przygotować się do działania po ewentualnym ataku. Reagowanie post factum to dziś za mało. Potrzebne są polityki bezpieczeństwa, które przygotują nas na działanie po ewentualnym ataku. Ten aspekt był zbyt długo traktowany po macoszemu, a to niestety są dziś bardzo częste przypadki. Obecnie musimy tworzyć polityki bezpieczeństwa, które w sposób ciągły będą kontrolować nasze przygotowanie do cyberataku.

Próby zaadresowania zagadnienia ryzyka związanego z ICT były podejmowane zarówno przez państwa członkowskie, jak i organy unijne. Proponowane roz-

wiązania regulowały dotąd problematykę ICT szczątkowo. Były też zbyt ogólne, pozostawiając organom krajowym dużą swobodę interpretacji. Brak jednolitej polityki w tym zakresie doprowadził do niespójności wymogów prawnych oraz powielania się przepisów w prawie unijnym i w porządkach krajowych. Instytucje finansowe operujące transgranicznie narażone są w związku z tym na ryzyka związane z koniecznością uwzględniania odmiennych regulacji, w zależności od rodzaju działalności oraz lokalnych wymogów w zakresie ICT. Zmienić ma to wspomniana DORA.

Jak te działania – zarówno na poziomie poszczególnych państw, jak i całej Unii Europejskiej – przekładają się na podejście do cyberbezpieczeństwa w poszczególnych organizacjach?

W efekcie tych działań cyberbezpieczeństwo stało się jednym z trzech głównych priorytetów zarządów. Kierowane przez nich organizacje muszą zawczasu przygotować się do działania po ewentualnym ataku. Reagowanie post factum to dziś za mało. Potrzebne są polityki bezpieczeństwa, które przygotują nas na działanie po ewentualnym ataku. Ten aspekt był zbyt długo traktowany po macoszemu, a to niestety są dziś bardzo częste przypadki. Obecnie musimy tworzyć polityki bezpieczeństwa, które w sposób ciągły będą kontrolować nasze przygotowanie do cyberataku.

Jak DORA może zmienić podejście do cyberbezpieczeństwa w sektorze finansowym?

Rozporządzenie to wprowadza – jako nadrzędną zasadę – pełną odpowiedzialność organu zarządzającego za określenie, zatwierdzenie, wdrożenie i nadzorowanie ram zarządzania ryzykiem związanym z ICT. Przejawia się to w szczególności w obowiązku opracowania i zatwierdzenia odpowiednich polityk, ustalenia ról i obowiązków związanych z ICT, określenia poziomu tolerancji ryzyka związanego z ICT, zatwierdzenia planów audytu oraz kontrolowania ustaleń dotyczących zewnętrznych dostawców usług ICT. To diametralna zmiana w porównaniu do tego, z czym mieliśmy do czynienia do tej pory. Z historii korporacyjnej narracja zmienia się w opowieść osobistą, konkretnego CIO, CTO, CSO, COO...

> W aspekcie cyberbezpieczeństwa kluczowa jest zarówno wiedza prawnicza, jak i technologiczna. Bardzo ważne jest, aby nasi klienci byli świadomi aspektów związanych z cyberbezpieczeństwem nie tylko od strony regulacyjnej – w czym pomóc może kancelaria Kochański & Partners – ale i technologicznej, np. w zakresie stosowania rozwiązań cloud computing. Tu ogromną rolę do odegrania mają eksperci firmy MAIN, z którą współpracujemy zarówno przy projektach u naszych klientów, jak i w ramach MAIN Partner Community, m.in. w zakresie programu „Bezpieczny Zarząd – Dyrektor IT".

W jaki sposób organizacje powinny przygotować się z jednej strony do nowych wyzwań związanych z cyberbezpieczeństwem, a z drugiej – przygotowywanych regulacji?

Po pierwsze, zmienić się muszą relacje z kluczowymi dostawcami uwzględniające nowe wymogi bezpieczeństwa IT. Po drugie, zmiany wymaga proces zakupowy. Już w czasie postępowania zakupowego powinniśmy weryfikować dostawcę pod kątem cyberbezpieczeństwa.

W tym aspekcie kluczowa jest zarówno wiedza prawnicza, jak i technologiczna. Pod względem nowych regulacji zweryfikować trzeba: zapisy w umowach, obowiązki przyszłego partnera, zakres jego odpowiedzialności za ewentualny wyciek, wiedzę i umiejętności pracujących po stronie firmy zewnętrznej zespołów, poziom oferowanego SLA, jak również określić potencjalne luki bezpieczeństwa. Ważne są tu także aspekty otwartości proponowanej technologii. Z tej perspektywy należy patrzeć nie tylko na dotychczasowe, ale i przyszłe umowy.

Trzeci aspekt, który należy brać pod uwagę, przygotowując się do nowych wyzwań związanych z nowymi regulacjami w zakresie cyberbezpieczeństwa, to sprawa dokumentacji wewnętrznej. Obejmuje to np. regulaminy związane z zakupami czy dostępem do strategicznych dla danej organizacji obiektów, np. centrów przetwarzania danych. Często powstawały one w czasie, gdy nie myślano o tak intensywnej cyfryzacji, a cyberbezpieczeństwo nie stanowiło tak newralgicznego aspektu funkcjonowania firm.

Coraz częściej warto także rozważyć posiadanie polisy ubezpieczeniowej, obejmującej skutki ewentualnego cyberataku. Firm oferujących tego typu polisy jest dziś dużo, ale trzeba wiedzieć o czym i jak rozmawiać z ich przedstawicielami. Może się okazać, że nie dostaniemy odszkodowania, bo nienależycie sprawdziliśmy dostawcę. Warto podkreślić, że pozwala ona nie tylko otrzymać środki z odszkodowania, lecz także pokazuje audytującym nas instytucjom, że nie traktujemy lekko sprawy cyberbezpieczeństwa, że dokładamy najwyższej staranności związanej z cyberbezpieczeństwem.

Wspominasz, że w opisywanych przez Ciebie aspektach kluczowa jest zarówno wiedza prawnicza, jak i technologiczna...

To prawda! Bardzo ważne jest, aby nasi klienci byli świadomi aspektów związanych z cyberbezpieczeństwem zarówno od strony regulacyjnej – w czym pomóc może kancelaria Kochański & Partners – jak i technologicznej, np. w zakresie stosowania rozwiązań cloud computing. Tu ogromną rolę do odegrania mają eksperci firmy MAIN, z którą współpracujemy nie tylko przy projektach u naszych klientów, ale też w ramach MAIN Partner Community, m.in. w zakresie programu „Bezpieczny Zarząd – Dyrektor IT".

Dobre przygotowanie jest o tyle ważne, że polskie oraz europejskie firmy i instytucje będą z tego rozliczane. Nie można już spraw bezpieczeństwa zamiatać pod dywan. Temat ten będzie istotny przez wiele lat. Proces przestawiania się organizacji na nowe tory – gdzie cyberbezpieczeństwo jest integralną częścią wszystkich procesów – będzie trwał.

Na czym polega współpraca kancelarii Kochański & Partners z MAIN?

Chcemy wspólnie wesprzeć klientów w tym, aby zestaw podjętych przez nich przed cyberatakiem działań maksymalnie zminimalizował jego ryzyko. Przeprowadzamy więc wspólne działania związane z audytami, szkoleniami i akcjami uświadamiającymi, jakie zmiany regulacyjne ich czekają. Odbywa się to w ramach programu „Bezpieczny Zarząd – Dyrektor IT". Program składa się z usług prawnych, których celem jest:

- zwiększenie bezpieczeństwa prawnego Klienta na wypadek incydentu bezpieczeństwa (potocznie cyberataku),
- wykazanie – na wypadek audytu wew. lub zew. okoliczności, w jakich doszło do incydentu bezpieczeństwa – podjęcia przez kadrę kierowniczą Klienta wymaganych aktów staranności, w celu zabezpieczenia informatycznego kierowanego przedsiębiorstwa.

Usługi mogą być świadczone kompleksowo lub punktowo – w zależności od życzenia Klienta.

Widać, że rośnie rola cyberbezpieczeństwa w strategiach działających w Polsce organizacji. Coraz ważniejsze staje się dla nich pokazanie swoim klientom, że strategia i procedury związane z bezpieczeństwem IT nie są tylko spisane na papierze, ale zostały wdrożone przez sprawdzonych doradców prawnych i technologicznych.

Co warto podkreślić, bez współpracy prawników i specjalistów IT trudno przekazać klientom realną, wartościową wiedzę. Dopiero to, co przekazujemy wspólnie z MAIN, stanowi spójną historię. Przykładowo wejście do chmury instytucji sektora finansowego wymaga analizy ryzyka nie tylko od strony prawnej, ale – może przede wszystkim – właśnie technicznej.

Wywiad przeprowadził
ADAM JADCZAK