CYBER-COMPLIANCE W CIENIU PANDEMII STUDIUM PRZYPADKU CYBER-OSZUSTWA

Prowadzenie biznesu w czasach kryzysu sanitarnego, w tym zmiana trybu pracy na zdalny, poszerzyły możliwości do popełniania przestępstw przez cyberprzestępców. Cyberprzestępcy coraz umiejętniej wykorzystują nowe technologie i inżynierię społeczną, wiedząc, że powodzenie ich działań zależy od błędu ludzkiego. Cyberatak może prowadzić do dotkliwych strat dla przedsiębiorstwa, np. gdy dochodzi do wyłudzenia pieniędzy. Dlatego warto przyjrzeć się zasadom cyber-bezpieczeństwa obowiązującym w organizacji, aby zmniejszyć ryzyko strat.

Cyberbezpieczeństwo w dobie pandemii

Od początku pandemii odnotowano **istotny wzrost cyberprzestępstw**, wśród których należy wymienić:

> **przełamywanie zabezpieczeń i kradzież danych** i informacji poufnych;

> **szantaż przy wykorzystaniu ransomware**, a więc programów komputerowych, które blokują dostęp do danych, stanowiących własność przedsiębiorstwa szantażowanego lub uniemożliwiają prawidłowe funkcjonowanie przedsiębiorstwa. Najświeższym przykładem w tym obszarze jest cyberatak na wysoko zdigitalizowany rurociąg Colonial Pipeline w USA;

> **wyłudzanie pieniędzy** poprzez przekierowanie strumienia płatności przeznaczonej dla kontrahenta, na rachunek bankowy w innym banku (nienależący do kontrahenta).

W odniesieniu do ostatniej kategorii incydentów – dochodzi do nich w związku z wykorzystaniem cyberprzestrzeni i narzędzi informatycznych, w szczególności tych służących ingerencji w komunikację elektroniczną (business e-mail compromise), w połączeniu z inżynierią społeczną. Efektem jest podszycie się np. pod kontrahenta czy dyrektora z wewnątrz organizacji.

W dobie pandemii – kiedy uwaga przedsiębiorców jest skupiona na utrzymaniu rentowności prowadzonej działalności,, odrabianiu strat, czy utrzymywaniu dobrych relacji z klientami – ostrożność często nie jest priorytetem, a przestępcy potrafią to umiejętnie wykorzystać. Newralgicznym momentem, który sprzyja cyberatakom, może być także wychodzenie z pandemii i towarzyszący temu entuzjazm. W tych właśnie okolicznościach, przedsiębiorca powinien zwrócić szczególną uwagę na kwestie cyber-bezpieczeństwa swojej organizacji.

Odstąpienie od dotychczasowych zasad (procedur) lub ich brak, może doprowadzić do niepożądanych skutków – zarówno finansowych, prawnych (np. w przypadku wycieku danych personalnych) jak i reputacyjnych. Konsekwencje mogą także ponosić poszczególne osoby z organizacji.

Dlatego warto przyjrzeć się, czy i jak w przedsiębiorstwie (w organizacji) stosowane są zasady cyber-compliance, które powinny wyeliminować ryzyka dokonania płatności na rzecz oszustów, co wielokrotnie przebiega według niżej przedstawionego scenariusza.

(Trywialne?) studium przypadku

Dwóch kontrahentów (na potrzeby studium przyjmujemy, że są to kontrahenci zagraniczni) pozostaje w stałych relacjach biznesowych, w ramach których Kontrahent 1 nabywa dobra (towary) niezbędne do jego działalności produkcyjnej od Kontrahenta 2. Płatności za dostawę towarów następują na podstawie faktury, przysyłanej w formie elektronicznej, przelewem bankowym na wskazywany na fakturze rachunek bankowy. Jest to rachunek bankowy, który od lat pozostaje niezmieniony. Korespondencja dotycząca płatności odbywa się mailowo, a osoby, które po obu stronach odpowiedzialne są za kwestie finansowe, pozostają w stałym kontakcie, niekiedy wręcz koleżeńskim.

W związku ze znaczącym zamówieniem na dostawę towarów, zostaje wystawiona faktura na wysoką kwotę. Zbliża się termin płatności faktury i Kontrahent 1 otrzymuje wiadomość, z adresu – wydawałoby się – Kontrahenta 2 z zapytaniem, kiedy zostanie dokonana płatność, i **jednocześnie z prośbą o to, aby przelew należności z tytułu faktury został dokonany na inny rachunek bankowy**. Jako powód zmiany, wskazywany jest audyt, jakiemu akurat zostało poddane konto bankowe służące do rozliczeń między kontrahentami.

Rachunek bankowy, jaki zostaje wskazany, jest prowadzony (ponownie na potrzeby studium) przez bank z siedzibą w Polsce, państwie, które nie wykazuje żadnego związku z relacjami gospodarczymi między kontrahentami. Styl i poprawność językowa wiadomości informującej o zmianie rachunku bankowego nie budzą wątpliwości, bowiem w stosunku do poprzedniej korespondencji nie zachodzą żadne zmiany. Adres mailowy, z jakiego przychodzą wiadomości, także na pierwszy rzut oka, nie wzbudza wątpliwości.

Po przekazaniu nowego rachunku bankowego do Kontrahenta 1 przychodzi ciąg wiadomości z pytaniem, kiedy przelew zostanie wykonany, i prośbą o przesłanie jego potwierdzenia.

Realizacja przelewu zostaje zlecona bankowi obsługującemu Kontrahenta 1 i środki pieniężne zostają wysłane.

To, czy dojdzie do poniesienia szkody, zależy od tego, jak szybko Kontrahent 1 zorientuje się, że doszło do oszustwa, oraz reakcji banku prowadzącego rachunek, na który wpłynęły pieniądze.

Powyżej opisany scenariusz może mieć wiele wariantów. To, jak daleko posunięta jest narracja uwiarygadniająca oszustwo, może wynikać między innymi z tego, jak daleko była posunięta ingerencja w system informatyczny przedsiębiorstwa i jak długo trwała.

Diagnoza: jak do tego doszło?

Wydawałoby się – scenariusz trywialny. Nic bardziej mylnego. Jego realizacja jest wynikiem zastosowania przez cyberprzestępców szeregu mechanizmów, które prowadzą do decyzji negatywnej w skutkach dla przedsiębiorstwa.

Przede wszystkim – cyberprzestępcy dokonują przełamania zabezpieczeń systemu informatycznego. Umożliwia to obserwację działalności organizacji od wewnątrz i pozyskanie wiedzy o sposobie jej funkcjonowania, istotnych transakcjach; także o tym, że organizacja może znajdować się w newralgicznym momencie jej działalności operacyjnej lub korporacyjnej, jak np. wizyta CEO regionu lub zamknięcie ksiąg rachunkowych, co może wywoływać poczucie presji, skutkującej z kolei obniżeniem czujności w odniesieniu do innych sfer działalności przedsiębiorstwa. Przełamanie zabezpieczeń systemu informatycznego

pozwala, także sprawcom, przyjrzeć się komunikacji pomiędzy przedsiębiorstwem a kontrahentem w zakresie rozliczeń z tytułu transakcji.

Pozyskanie wiedzy o przedsiębiorstwie pozwala cyber-oszustom wkroczyć w korespondencję mailową, dotyczącą płatności w odpowiednim momencie. Dochodzi do przejęcia kontroli nad komunikacją, w tym do podstawiania wiadomości e-mail i ingerowania w ich treść.

Manipulacja korespondencją mailową odbywa się często przy wykorzystaniu, tworzonych na potrzeby oszustwa, **adresów mailowych, łudząco podobnych do adresów**, wykorzystywanych przez rzeczywistych kontrahentów. Różnice w adresach mailowych potrafią być trudno dostrzegalne. Przykładowo – „i" pisane majuskułą zastępowane jest literą „L" pisaną minuskułą, usunięcie myślnika między dwoma członami rozwinięcia adresu mailowego, dodanie jednej litery na końcu ostatniego członu w rozwinięciu adresu e-mail, zastąpienie skrótu „.com" innym skrótem zgodnym z kontekstem, np. „.eu", lub „.pl".

Są to zmiany trudno dostrzegalne, zwłaszcza, przy towarzyszącym relacjom biznesowym tempie. Niejednokrotnie zdarza się też tak, że wskutek ingerencji w system informatyczny, cyberprzestępcy przejmują kontrolę nad adresem mailowym, wykorzystywanym rzeczywiście przez kontrahenta.

Cyberprzestępcy są w stanie także obejść wymagania, jakie mogą wynikać choćby z wewnętrznych procedur księgowych, np. wystawienia faktury zawierającej nowy rachunek bankowy lub potwierdzenia przez kadrę zarządczą kontrahenta, że rachunek bankowy został zmieniony. Praktyka pokazuje, że dokumenty takie są podrabiane, co w dobie digitalizacji nie sprawia niestety większego problemu, zwłaszcza jeżeli obserwacja działalności przedsiębiorstwa przez przestępców była pogłębiona.

Obok nowych technologii, cyber-oszuści umiejętnie wykorzystują inżynierię społeczną, zdając sobie sprawę z tego, że powodzenie ich działań zależy od błędu ludzkiego. Wiedza na temat organizacji pozwala wykorzystywać elementy presji, jaka może spoczywać na osobie, będącej decydentem w zakresie rozliczeń, lub koleżeński kontekst relacji między osobami, które odpowiedzialne są za rozliczenia po stronie kontrahentów. Pandemia sama przez się, tworzy podatny grunt do manipulacji rzeczywistością.

Znaczenie mają więc cechy charakterystyczne komunikacji – styl, język. W jednej ze spraw ,sprawca podszywający się pod dyrektora finansowego kontrahenta, zadzwonił do dyrektora finansowego spółki, która była obowiązana do dokonania płatności, celem „potwierdzenia" zmiany rachunku bankowego. Według dyrektora wprowadzonego w błąd – głos tej osoby był właściwie taki sam, jak prawdziwego dyrektora finansowego kontrahenta.

Te wszystkie zabiegi prowadzą do uwiarygodnienia narracji o zmianie rachunku bankowego na rachunek prowadzony, nawet przez bank w państwie najbardziej egzotycznym w stosunku do realiów relacji gospodarczych, zwłaszcza tych utrwalonych. Niejednokrotnie dochodzi także do złamania wewnętrznych procedur w zakresie realizacji płatności (która np. mimo wymogu faktur w formie papierowej dokonywana jest na podstawie faktury przesłanej elektronicznie).

Środki zaradcze

Należy pamiętać, że szereg przedsiębiorstw, które zostały zaatakowane, jeszcze długo po ataku o tym nie wiedzą, a im więcej czasu upłynie od momentu nieuprawnionej ingerencji, tym większą szkodę może to wyrządzić przedsiębiorstwu.

W dzisiejszym świecie pytanie - czy stanę się przedmiotem cyberataku, jest pytaniem retorycznym.. Pytaniem istotnym jest natomiast: kiedy i w jaki sposób zostanę zaatakowany. **Dla zminimalizowania skutków cyberataków, istotne jest wprowadzenie i utrwalanie kilku podstawowych zasad:**

> **cyber-BHP (cyber-compliance),**

> **weryfikacji skuteczności systemów** zabezpieczenia informatycznego,

> **postępowania kryzysowego** w przypadku, kiedy dojdzie do ujawnienia, że organizacja stała się celem cyberataku.

W przypadku, kiedy przelew zostanie zrealizowany, a pieniądze zostaną zablokowane przez bank i związku z tym – powiadomione organy ściągania, organy mogą podjąć decyzję o rozpoczęciu postępowania karnego. Wówczas zasadne będzie zgłoszenie się do postępowania w charakterze strony. Takie zgłoszenie i nawiązanie dialogu z organem ścigania może przyczynić się do szybszego zwolnienia środków pieniężnych z zatrzymania i ich zwrotu na rzecz przedsiębiorstwa. Należy jednak mieć na względzie, że zwrot środków pieniężnych na rzecz pokrzywdzonego, może nastąpić po upływie kilku lub nawet kilkunastu miesięcy.

Dlatego – w ramach cyber-compliance i w granicach rozsądku – warto pamiętać i stosować zasadę, że jeżeli coś się wydaje podejrzane, to zapewne podejrzane jest, i w związku z tym należy to sprawdzić.

W przypadku pytań zapraszam do kontaktu.

Aleksandra Stępniewska – counsel, adwokat
aleksandra.stepniewska@wkb.pl