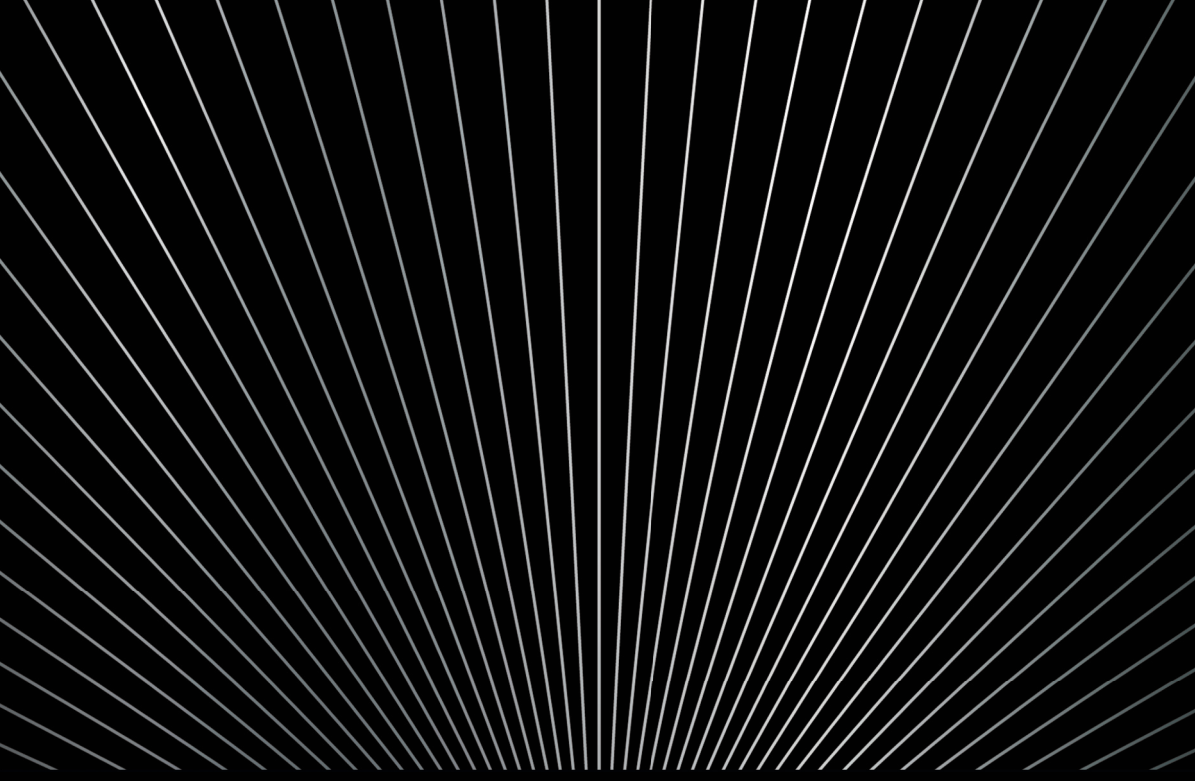

JAKUB BOJANOWSKI

ZDĄŻYĆ PRZED HAKEREM

JAK PRZYGOTOWAĆ FIRMĘ NA CYBERATAK

mt biznes

Spis treści

Wstęp

W dzisiejszych czasach ani w życiu prywatnym, ani zawodowym nie możemy się obyć bez technologii. Pandemia COVID-19 spowodowała, że nawet najwięksi technosceptycy zostali zmuszeni do korzystania z komputerów i sieci. Technologia uratowała miejsca pracy i firmy – bez możliwości kontaktu, telekonferencji czy wymiany dokumentów przez sieć wiele instytucji byłoby zmuszonych do całkowitego zaprzestania swojej działalności.

Podczas pandemii, w miarę jak kolejne instytucje w coraz większym stopniu zaczynały prowadzić działalność z wykorzystaniem internetu, w sieci pojawiła się nowa grupa internautów, z reguły gorzej przygotowanych do bezpiecznego korzystania z sieci. Tym samym pandemia otworzyła cyberprzestępcom nowe możliwości działania na większą niż dotychczas skalę.

W rezultacie działalności cyberprzestępców jesteśmy bardziej niż kiedykolwiek wcześniej narażeni na próby oszustwa, wyłudzenia informacji lub środków finansowych czy kradzież tożsamości. Mimo że korzystanie z technologii w sposób bezpieczny ma coraz większe znaczenie, nasze zachowania w internecie (na co często zwracają uwagę socjologowie) można wiązać z tzw. paradoksem prywatności. Internauci głośno deklarują swoje dążenie do zachowania prywatności w sieci, ale w ślad za tą deklaracją nie idą praktyczne działania. Cha-

rakter publikacji dokonywanych przez typowego internautę w mediach społecznościowych (publikowanie zdjęć i informacji o życiu prywatnym) nie ma nic wspólnego z zachowaniem prywatności.

Bardzo podobny paradoks (nazwijmy go cyberparadoksem) możemy zaobserwować w odniesieniu do bezpieczeństwa informacji w sferze biznesu. Firmy i zarządzający nimi menedżerowie głośno deklarują, że zagrożenia z zakresu cyberbezpieczeństwa są jednymi z najważniejszych wyzwań biznesowych, ale przyglądając się działaniom podejmowanym w celu zapobiegania cyberincydentom, możemy zauważyć, że nie zawsze te deklaracje przekładają się na konkretne działania praktyczne.

Zapewnienia menedżerów o priorytetowym podejściu do cyberbezpieczeństwa rzadko są odzwierciedlane w tematyce spotkań zarządów lub rad nadzorczych. Nawet wśród liderów rynku, w przypadku których poziom bezpieczeństwa informatycznego jest na odróżniającym ich od innych poziomie, udział menedżerów w zarządzaniu tym obszarem często ogranicza się do powołania szefa ds. bezpieczeństwa informacji (ang. *Chief Information Security Officer* – CISO) i zdelegowaniu na niego wszystkich decyzji.

Cyberparadoks przejawia się w tym, że zarządy wolą koncentrować się na tradycyjnych zagadnieniach menedżerskich, takich jak finanse, sprzedaż czy działalność operacyjna. Oceniając zarząd, który temat zachowania płynności finansowej spółki w całości zdelegował na szefa działu finansów i nie interesuje się stanem rachunku bankowego, uznalibyśmy go za niedostatecznie wykonujący swoje obowiązki. Analogiczna postawa zarządu w odniesieniu do (zgodnie z deklaracjami – priorytetowego obszaru) cyberbezpieczeństwa nie tylko nie razi, lecz nawet jest praktycznym standardem.

Jednym (choć na pewno nie jedynym) czynnikiem, który przyczynia do cyberparadoksu, jest bariera komunikacyjna, która utrudnia menedżerom dotarcie do praktycznych informacji na temat tego, w jaki sposób mogą włączyć się w zarządzanie cyberbezpieczeństwem.

Mimo że o cyberbezpieczeństwie mówi się dużo i szeroko, komunikaty, które docierają do typowego menedżera, ciężko jest wykorzystać do zbudowania rzetelnej wiedzy na ten temat, tak aby móc przełożyć ją na konkretne działania zarządcze.

Media, podejmując tematykę cyberbezpieczeństwa, najczęściej skupiają się na szczególnie spektakularnych incydentach dotyczących największych korporacji lub czołowych instytucji sektora publicznego. Incydenty nagłaśniane w mediach mogą na tyle przerażać skalą swoich skutków, że potencjalny atak hakerów, jako rzeczywiste zagrożenie, jest przez menedżerów niejako wypierany (podobne wyparcie zachodzi w odniesieniu do katastrof naturalnych – w praktyce nikt nie wierzy, że jego dom lub miejsce pracy będzie zniszczone w wyniku pożaru lub powodzi). W przekazie medialnym w dalszym ciągu umyka fakt, że różne formy cyberataków są obecnie coraz bardziej powszechne i dotyczą praktycznie każdego, choć nie zawsze wiążą się z incydentami na ogromną skalę.

Do zainteresowania zarządzających instytucjami tematyką cyberbezpieczeństwa nie przyczyniają się także eksperci techniczni, którzy nie tylko posługują się hermetycznym i specjalistycznym żargonem, lecz także zazwyczaj koncentrują uwagę na zagadnieniach technicznych związanych z zabezpieczaniem poszczególnych systemów. Analizując dyskusje środowiska specjalistów na temat znanych cyberincydentów, widzimy, że dominującym tematem jest sposób realizacji określonego cyberataku, a nie skutków, jakie wywołał on dla działalności instytucji będącej jego ofiarą, czy reakcji na ten incydent.

Rezultatem bariery komunikacyjnej, której doświadczają menedżerowie (w większości specjaliści od finansów, sprzedaży czy produkcji, a nie technologii), jest decyzja o pozostawieniu zagadnień cyberbezpieczeństwa jako „domeny wyłącznie dla fachowców". Szefowie, którzy nie czują się komfortowo, podejmując dyskusję na tematy techniczne z fachowcami i bojąc się zarzutu braku kompetencji, pozostawiają specjalistom od bezpieczeństwa szeroką (szerszą niż w innych obsza-

rach zarządzania) autonomię działania. W organizacjach, gdzie na stanowisko CISO powołano osobę, która ma kompetencje i możliwości organizacyjne do samodzielnego podejmowania decyzji, taki podział zadań niekoniecznie musi być problemem, ale w większości instytucji i w dłuższej perspektywie czasu rozwiązanie takie prowadzi do pogłębienia cyberparadoksu.

> W trakcie swojej ponaddwudziestoletniej kariery zawodowej jako doradca zajmujący się bezpieczeństwem informatycznym miałem okazję współpracować zarówno z ekspertami od cyberbezpieczeństwa, jak i ich przełożonymi – członkami zarządów firm o różnej wielkości, reprezentujących prawie wszystkie sektory gospodarki. Moje doświadczenia wskazują, że bariera informacyjna stojąca u podstaw cyberparadoksu jest możliwa do przełamania i że o wielu zagadnieniach z obszaru cyberbezpieczeństwa możemy dyskutować, bazując na swoich ogólnych doświadczeniach w zarządzaniu, nawet jeżeli nie jesteśmy ekspertami technicznymi. Ogólna wiedza menedżerska i doświadczenie zawodowe zarządzających stanowią doskonałą podstawę do tego, aby obszar bezpieczeństwa informacji traktować na równi z innymi obszarami biznesowymi. A podstawy wiedzy technicznej leżące u fundamentów cyberbezpieczeństwa nie są tak trudne, jak to się powszechnie uważa.

Ten pogląd i pokusa, aby podjąć próbę przełamania bariery informacyjnej na temat cyberbezpieczeństwa stoją u podstaw mojej decyzji o napisaniu tej książki. Jako tematykę wybrałem kilka zagadnień z zakresu zarządzania cyberbezpieczeństwem – takich, które nie wymagają wiedzy specjalistycznej, a jednocześnie ilustrują związek między technologią informatyczną i nowoczesnym biznesem. Cyberbezpieczeństwo jest pokazane z perspektywy procesów zarządczych, standardów dobrej praktyki i wybranych regulacji.

Po zapoznaniu się z treścią książki czytelnicy – menedżerowie (i przyszli menedżerowie) – nie zostaną ekspertami od cyberbezpieczeństwa, ale mam nadzieję, że zdobędą ogólną

wiedzę, która pozwoli im nawiązać dialog z ekspertami, a w razie potrzeby zadać kilka trafnych pytań na temat toczącego się projektu lub przedstawianego do akceptacji budżetu.

Mając na uwadze grupę docelową czytelników, starałem się pisać książkę w sposób wolny od żargonu technicznego, ale oczywiście omawianie cyberbezpieczeństwa przy całkowitym ignorowaniu kwestii technologicznych nie jest możliwe. Poszczególne terminy fachowe są wprowadzane stopniowo i w miarę możliwości wyjaśniane na bieżąco. Dodatkowo są one wyjaśnione w słowniku zawartym na końcu książki. Trudniejsze i bardziej zaawansowane kwestie techniczne są albo pominięte, albo w nieco uproszczony sposób wyjaśnione w załącznikach.

W tekście starałem się skoncentrować na prezentacji praktycznych rozwiązań, a nie wiedzy teoretycznej czy obowiązujących przepisach prawa. Oczywiście omówiłem główne regulacje dotyczące bezpieczeństwa informacji, z którymi czytelnicy mogą zetknąć się w swojej praktyce zawodowej, ale uważam, że ważniejsze są wyzwania przy ich wdrożeniu, a nie analizowanie poszczególnych przepisów czy szczegółowych zaleceń.

Kluczowy był dla mnie praktyczny aspekt książki jako poradnika dla menedżerów i formy dzielenia się doświadczeniami. Prezentowane zagadnienia starałem się zilustrować poprzez przykłady oparte na moich doświadczeniach zawodowych i studium przypadku, które pojawia się w kolejnych rozdziałach. Oczywiście wykorzystane przeze mnie w przykładach problemy biznesowe zostały zanonimizowane i tak zmodyfikowane co do szczegółów, aby nie było możliwe ustalenie, do jakiej instytucji odnoszą się opisane sytuacje. W tych sytuacjach, gdzie podawana jest konkretna nazwa instytucji, wykorzystane zostały wyłącznie informacje publicznie dostępne w mediach. Kilka z wykorzystanych przykładów zostało stworzonych wyłącznie na potrzeby książki. Firma FFG, która stanowi bazę do studium przypadku, jest całkowicie fikcyjna. Architektura systemów i poszczególne problemy biznesowe omawiane w tym studium przypadku stanowią kompilację

rozwiązań spotykanych na rynku, ale sposób, w jaki zostały one wykorzystane w książce, nie odpowiada żadnej konkretnej instytucji.

Wybór tematów i kolejność rozdziałów w książce mają ułatwić czytelnikowi stopniowe przejście od roli nieświadomej ofiary potencjalnego cyberataku do roli lidera, który jest w stanie aktywnie stawić czoła sytuacji kryzysowej. Wykorzystując jako tło dość typowy incydent, próbujemy zrozumieć, w jaki sposób na cyberzagrożenia reagują menedżerowie, którzy po raz pierwszy mają do czynienia z atakiem hakerów. Następnie stopniowo budujemy wiedzę na temat cyberbezpieczeństwa i poznajemy zasady ochrony informacji pozwalające przeciwdziałać atakom, a przynajmniej wykrywać je na tyle wcześnie, aby móc ograniczyć ich potencjalne skutki.

Rozpoczynamy od prezentacji „krajobrazu cyberzagrożeń" – wytłumaczenia, kim są typowi cyberprzestępcy i jakie są ich cele i sposób działania. Pokazujemy, w jaki sposób kierownictwo instytucji może wykorzystać te informacje do budowania firmowego programu cyberbezpieczeństwa. Wykorzystując znane na rynku standardy i regulacje, prezentujemy narzędzia menedżerskie pozwalające na stworzenie ram organizacyjnych, na bazie których menedżerowie mogą nadzorować działania podejmowane przez fachowców w celu podniesienia bezpieczeństwa teleinformatycznego.

W następnej części książki (w dalszym ciągu bez wchodzenia w szczegóły techniczne) staramy się wyjaśnić najważniejsze obecnie wyzwania charakterystyczne dla gospodarki elektronicznej: zapewnienie bezpiecznego obrotu finansowego sieci i zachowanie prywatności przez internautów korzystających z handlu elektronicznego. Staramy się pokazać, w jaki sposób tematyka ochrony danych osobowych, która zyskała dużą popularność dzięki wejściu w życie RODO, może być wykorzystana do budowania firmowego systemu cyberbezpieczeństwa.

Ostatnia część książki jest poświęcona czarnym scenariuszom – reagowaniu na cyberincydenty i zarządzaniu w sytu-

acji kryzysowej, gdy zarządzana przez nas instytucja stała się celem cyberataku. Nie podajemy tutaj czytelnikom gotowych metod postępowania w tego typu sytuacjach, ale staramy się pokazać, w jaki sposób wiedza zdobyta podczas lektury książki może być pomocna w tej trudnej sytuacji.

> Liczę na to, że dzięki lekturze tej książki czytelnicy będą w stanie „zdążyć przed hakerem" i łącząc zawarte w niej informacje ze swoją intuicją i doświadczeniem menedżerskim, przygotować się do potencjalnego kryzysu tak, aby – gdy będzie to konieczne – pokazać się w roli skutecznego lidera.

Podziękowania

Korzystając z okazji, chciałbym podziękować osobom, które przyczyniły się do powstania tej książki. U podstaw jej napisania leży moja współpraca z Akademią Leona Koźmińskiego, gdzie w ramach programu Master in Big Data Science prowadziłem autorski program zajęć na temat cyberbezpieczeństwa. Program zajęć i uwagi ze strony studentów leżą u podstaw pierwotnej koncepcji książki. Chciałbym podziękować im za aktywny udział w prowadzonych przeze mnie zajęciach, który pozwolił mi na spojrzenie na cyberbezpieczeństwo z innej, zupełnie nowej dla mnie perspektywy. Dziękuję także **profesorce Anecie Hryckiewicz-Gontarczyk**, która zaprosiła i zachęciła mnie do udziału w tym programie w nowej dla mnie roli wykładowcy akademickiego.

Do napisania książki zainspirował mnie **profesor Ryszard Buczyński**. Dziękuję mu za przedstawienie mi perspektywy doświadczonego pracownika naukowego, która była pomocna w podjęciu decyzji o napisaniu książki.

Moją wiedzę i doświadczenie z zakresu cyberbezpieczeństwa, które zawarłem w książce, budowałem przez ponad 20 lat pracy w firmie doradczej Deloitte, w której miałem przyjemność współpracować z wieloma utalentowanymi koleżankami i kolegami. Wszyscy oni na pewno przyczynili się do powstania tej książki, ale troje z nich miało tu rolę szczególną.

Współpraca z **Marcinem Ludwiszewskim**, z którym przez ponad cztery lata rozwijaliśmy zespół Cyber w Deloitte, pozwoliła mi na spojrzenie na kwestie cyberbezpieczeństwa ze znacznie szerszej perspektywy. Dzięki Marcinowi nauczyłem się, w jaki sposób na temat cyber skutecznie rozmawiać z kadrą menedżerską i jak wygląda dyskusja na temat cyberbezpieczeństwa w międzynarodowych instytucjach, w których Marcin spędził znaczącą część swojej kariery zawodowej. Konsultowałem z nim niektóre fragmenty tekstu i to jego uwagi pozwoliły na to, aby w książce zachować dobre proporcje pomiędzy teorią i praktyką.

Adam Haertle – także dawny kolega z Deloitte, a obecnie szef serwisu `ZaufanaTrzeciaStrona.pl` zainspirował mnie jako najlepszy w Polsce ekspert od popularyzacji tematyki cyberbezpieczeństwa. Z bezpośredniej pomocy Adama i z jego serwisu korzystałem przy wynajdywaniu niektórych materiałów źródłowych i potwierdzaniu niektórych zawartych w przykładach informacji.

Agata Jankowska-Galińska, z którą konsultowałem się w niektórych kwestiach prawnych, pomogła mi w usystematyzowaniu wiedzy z zakresu RODO i zrozumieniu, jak skutecznie można połączyć perspektywę prawnika i informatyka przy projektowaniu bezpieczeństwa systemów informatycznych.

Dziękuję także **profesorce Katarzynie Śledziewskiej**, która podjęła się trudnej roli zrecenzowania książki i której uwagi pozwoliły mi na wyeliminowanie kilku ważnych luk w prezentowanych przeze mnie zagadnieniach.

Specjalną rolę we wspieraniu mnie w trakcie pisania książki mieli moja żona **Joanna Bojanowska** i dzieci **Ewa** i **Filip**. Dziękuję im za stałe zainteresowanie postępem prac i podtrzymywanie mojego zaangażowania podczas kilku miesięcy, które poświęciłem na napisanie książki. Ewa (jako jedyna osoba w naszej rodzinie, która nie jest zawodowym informatykiem) wspólnie z redaktorką **Anną Goryńską** pełniły ważną funkcję, pilnując, aby ostateczny tekst książki był zrozumiały także dla osób niebędących ekspertami technicznymi.

Pani Annie, która dbała o poprawność i czytelność tekstu, należą się szczególne podziękowania. Bez stałej zachęty z jej strony oraz wsparcia ze strony pana redaktora **Marka Rostockiego** znacznie trudniej byłoby mi zmierzyć się z wyzwaniem, jakim jest napisanie pierwszej, tak obszernej publikacji.

Rozdział 1

Menedżer w obliczu cyberincydentu

W czerwcu 2021 r. dochodzi do – jak dotychczas – najbardziej spektakularnego cyberincydentu w Polsce. Jeden z portali publikuje e-maile Szefa Kancelarii Prezesa Rady Ministrów. Skutkiem jest ujawnienie wewnętrznych dokumentów rządowych i poważny kryzys wizerunkowy. Przez kolejne miesiące stopniowo publikowane są kolejne dokumenty, które odsłaniają kolejne fakty na temat przyczyn i zasięgu incydentu.

Zasięg medialny incydentu był na tyle duży, że możemy założyć, iż każdy z czytelników nie tylko o nim słyszał, lecz także zapoznał się z różnymi komentarzami i opiniami ekspertów zawierającymi zarówno fakty, oceny, jak i spekulacje na temat tego zdarzenia. Dalsze piętnowanie oczywistych słabości, które zostały ujawnione przy okazji tego incydentu, nie jest intencją autora. Zamiast tego spróbujmy wykorzystać tę sytuację w sposób pozytywny – jako przykład, który skłoni nas do pomyślenia o tym, w jaki sposób możemy podnieść poziom naszego cyberbezpieczeństwa w systemach informatycznych wykorzystywanych przez nas na co dzień w życiu zawodowym i prywatnym.

Zakładam, że przynajmniej dla niektórych czytelników informacja o incydencie była okazją do osobistej refleksji na temat tego, co by się stało, gdyby podobna sytuacja zdarzyła się w odniesieniu do jego prywatnych danych albo gdyby miała

miejsce w instytucji, w której pracuje (lub którą kieruje). Tak szeroko nagłośniony incydent jest bardzo dobrą okazją do podjęcia dyskusji na temat cyberzagrożeń i można go wykorzystać na wielu poziomach:

- menedżera – jako argument pozwalający na wprowadzenie tematu cyberbezpieczeństwa do programu obrad zarządu czy rady nadzorczej;
- pracownika – jako ciekawy przykład do omówienia na szkoleniu z zakresu bezpieczeństwa informacji;
- specjalisty – jako przykładowy scenariusz pomocny przy weryfikacji, w jaki sposób w podobnej sytuacji sprawdziłyby się firmowe procedury komunikacji i zarządzania kryzysowego.

Analogie między incydentem a sytuacją, w której znajduje się dowolna instytucja, niezależnie od tego, czy działa w sektorze publicznym, czy jest firmą komercyjną, są bardzo silne. Tym bardziej, że tak naprawdę historia w KPRM nie była szczególnie wyjątkowa. Oficjalnie niewiele wiadomo na temat szczegółów technicznych samego włamania, a w zalewie spekulacji ciężko jest ocenić, które z publikowanych informacji są rzetelne, a które stanowią *fake news*. Dotychczas jednak żadne doniesienia nie wskazują na to, że za incydentem stoi jakaś wyrafinowana wiedza lub technologia. Jego przyczyną było sprzęgnięcie się ze sobą nie najlepszych praktyk w eksploatacji rozwiązań technologicznych.

Rzetelna refleksja i zaakceptowanie, że w każdej instytucji można zaobserwować takie słabości, jakie wystąpiły w KPRM, są początkowym etapem budowania świadomego programu ochrony przez cyberprzestępcami. Wróćmy więc na chwilę do postaw i zachowań, które zostały ujawnione podczas omawianego cyberincydentu, ale oceńmy je nie przez pryzmat zdarzeń komentowanych przez media, a przez analogię do praktyki biznesowej, którą możemy zaobserwować w każdej (także naszej) instytucji.

Zaklinanie rzeczywistości

> Przekonanie, że działalność naszej instytucji jest na tyle nieinteresująca dla cyberprzestępców, że nie powinniśmy się spodziewać ataku, nie jest może prawidłowym założeniem w odniesieniu do KPRM, ale leży u podstaw zaniedbań w budowaniu programu cyberbezpieczeństwa także w wielu innych instytucjach.

Pierwszy i podstawowy błąd popełniany przez większość ofiar ataków cybernetycznych to bagatelizowanie zagrożenia, jakim jest działalność cyberprzestępców. W sytuacji, w której mamy świadomość, że działalność hakerów pozostaje poza naszą kontrolą, ignorowanie informacji na temat cyberzagrożeń daje nam pozorne poczucie komfortu. Alternatywą dla tego względnego spokoju jest stałe poczucie zagrożenia ze strony cyberprzestępców. Dlatego większość z nas odrzuca scenariusze, w których jesteśmy celem ataku hakerskiego.

Taką postawę przyjmujemy zarówno w życiu prywatnym (nie uruchamiając nawet podstawowych zabezpieczeń na wykorzystywanych przez nas urządzeniach technicznych: telefonie, tablecie czy domowym komputerze), jak i zawodowym (nie wdrażając kompleksowego programu ochrony przed cyberatakiem).

Ciągłe doniesienia medialne na temat kolejnych incydentów zamiast stanowić ostrzeżenie, często paradoksalnie wzmacniają bierne podejście do cyberzagrożeń. W sytuacji, w której media w naturalny dla nich sposób koncentrują się na najbardziej spektakularnych incydentach, łatwo jest dojść do wniosku, że ataki hakerów są domeną filmów szpiegowskich lub sensacyjnych i nie dotyczą zwykłej firmy czy statystycznego Kowalskiego. Scenariusz brzemiennego w skutkach włamania do systemów, gdzie wykradane są ważne dane albo unieruchamiane kluczowe systemy, wydaje się dla typowego odbiorcy całkowicie nierealny. Wywołuje zainteresowanie, ale nie obawę o własne dane czy systemy.

W rzeczywistości zagrożenia cybernetyczne są powszechne. Sprawcy (czy, jak mówią fachowcy, „aktorzy") cyberincydentów mogą się rekrutować z różnych środowisk i w rezultacie ich ofiarami mogą być osoby i instytucje o różnym profilu. Oczywiście nie każdy zasługuje na to, aby być celem ataku ze strony obcych służb wywiadowczych, ale przyczyny cyberataków mogą być bardzo różne. Dość często zdarza się, że ataki lub drobniejsze incydenty cybernetyczne (szczególnie wobec większych korporacji) są reakcją grup społecznych (tzw. haktywistów) na negatywne wydarzenia medialne dotyczące firmy lub działaniem ze strony niezadowolonych pracowników. Wykradanie poufnych informacji przez konkurencję pozornie tylko jest domeną powieści sensacyjnych – zdarza się zaskakująco często. Mniejsze instytucje, które są na tyle małe, że pozornie nikt nie będzie się nimi interesował, są natomiast podatne na ataki połączone z szantażem i żądania okupu (które stanowią obecnie trend dominujący w cyberprzestępczości).

Deprecjonowanie skali incydentu

> Wspólną cechą pierwszych wypowiedzi decydentów po incydencie w KPRM była próba przedstawienia go jako niewielkiego w skutkach drobnego zdarzenia i argumentowania, że ujawnione informacje miały niewielkie znaczenie dla funkcjonowania rządu. Jest to bardzo typowa postawa, którą można zaobserwować w większości tego typu wydarzeń.

Świadomość, że zagrożenia są realne, pojawia się dopiero wtedy, kiedy stajemy się ofiarą skutecznego ataku, choć także na tym etapie dość często pojawiają się próby odrzucania faktów. Prezentowanie incydentu jako niewielkiego, bieżącego problemu, który szybko zostanie rozwiązany, jest na tyle powszechne wśród kadry zarządzającej, że można nawet pokusić się o wskazanie takiej postawy jako standardowej reakcji menedżerów na cyberincydenty.

Reakcja decydentów (kierownictwa) na sytuację kryzysową jest bardzo często papierkiem lakmusowym dla kultury organizacyjnej danej instytucji. Osoby prezentujące autokratyczny styl zarządzania i przyzwyczajone do znajdowania posłuchu wśród pracowników wpadają w typową pułapkę autorytetu. Próbują rozwiązać incydent przez posługiwanie się możliwością podejmowania decyzji i siłą wynikającą z zajmowanej pozycji. Takie podejście może sprawdzać się w sytuacjach, które mają swoje przyczyny wewnątrz organizacji (awarii sprzętu), gdzie łatwo jest wskazać osobę odpowiedzialną i wyciągnąć wobec niej konsekwencje, ale charakter cyberincydentów jest trochę inny niż typowej awarii. Incydent jest kontrolowany przez niepodatną na naciski kadry zarządzającej stronę zewnętrzną. W sytuacji, kiedy wskazanie przyczyn zdarzenia jako leżących wewnątrz organizacji nie jest możliwe dla obrony swojego wizerunku, prezes lub menedżer bardzo często realizuje strategię prezentowania incydentu jako wydarzenia niewielkiego w skutkach i o ograniczonym zasięgu. Taka narracja stopniowo zmienia się w czasie, w miarę jak narastające negatywne skutki wydarzenia uniemożliwiają jego dalsze deprecjonowanie. Kolejne zdarzenie ze scenariusza realizowanego przez hakerów wywołuje poczucie chaosu komunikacyjnego i generując dodatkowe straty wizerunkowe, dodatkowo przyczynia się do pogłębienia kryzysu.

Poszukiwanie łatwych rozwiązań

> W celu ograniczenia skutków incydentu podjęte zostały nieformalne kroki prawne, dzięki którym konto na publicznym serwisie udostępniające dane zostało zablokowane. Wyciągnięto także konsekwencje służbowe wobec jednego z pracowników.

Uzupełnieniem do wyciągania konsekwencji służbowych wobec „osób odpowiedzialnych" wewnątrz instytucji są próby analogicznych działań podejmowanych wobec podmiotów

z otoczenia zewnętrznego: dostawców usług, infrastruktury technicznej. Jako przyczyny kryzysu wskazywane są przyczyny leżące poza instytucją, a służby prawne podejmują próby rozwiązania incydentu na drodze prawnej, powiadamiając organy ścigania (czy przy większych incydentach służby państwowe).

Skuteczność tych tradycyjnych metod postępowania jest raczej niewielka, gdyż szybkie ustalenie sprawców cyberincydentu nie jest zazwyczaj możliwe. Nawet jeżeli wiemy, kto jest stroną atakującą, to wyciągnięcie wobec niej konsekwencji prawnych jest bardzo utrudnione.

Znacząca większość cyberincydentów ma charakter transgraniczny i ich aktorzy operują w krajach, gdzie albo system prawny podchodzi do cyberprzestępczości w sposób liberalny, albo organy ścigania nie są dostatecznie sprawne, aby reagować na incydenty na bieżąco.

Cechą charakterystyczną cyberprzestępczości jest to, że – nawet jeżeli działania prawne są skuteczne – to zazwyczaj ich sukces ma charakter tymczasowy. Usunięcie poufnych danych z publicznego serwisu lub zamknięcie serwerów, które były wykorzystane do ataku, pozwala na ograniczenie negatywnych skutków zdarzenia na krótką metę (w trakcie apogeum kryzysu), ale nie rozwiązuje sytuacji na przyszłość. Należy się spodziewać, że po krótkim okresie względnego spokoju cyberprzestępcy stworzą nowy kanał umożliwiający im kontynuowanie dotychczasowej działalności.

Trudności w analizie zdarzenia

> Bezpośrednio po publikacji korespondencji ministra nie wiedziano, jakie było źródło wycieku informacji. Częściowe informacje były dostępne, a sprawa została przekazana do zbadania odpowiednim służbom państwowym. Wiemy, że przygotowanie ataku trwało kilka lub kilkanaście miesięcy, ale ustalenie, jaka jest rzeczywista skala zdarzenia, jest bardzo trudne. Nie tylko dlatego, że informacje te zostaną zapewne utajnione.

Dla osób, które po raz pierwszy stykają się z cyberincydentem, bardzo dużym zaskoczeniem okazuje się fakt, że ustalenie, na czym tak naprawdę polegało zdarzenie, nie zawsze jest możliwe. Incydent obserwujemy przez skutki działania hakerów: nasze systemy mogą stać się niedostępne lub poufne dane mogą zostać ujawnione w internecie, ale wskazanie, co jest przyczyną tej sytuacji i w jaki sposób przestępcy uzyskali dostęp do naszej infrastruktury, może wykraczać poza nasze umiejętności techniczne.

Systemy informatyczne dają teoretyczną możliwość prowadzenia dzienników zdarzeń i są w stanie rejestrować informacje pozwalające na ustalenie potencjalnego źródła i sposobu ataku, ale po pierwsze dane te nie zawsze są dostępne, a po drugie ich analiza może być bardzo utrudniona. W sytuacji, kiedy atak hakerski obejmuje wiele serwerów będących w gestii różnych instytucji (które często są także współofiarami ataku), zebranie wszystkich dostępnych informacji i ich przeanalizowanie mogą wymagać dużej ilości czasu i zastosowania specjalistycznych narzędzi. Dla specjalistów nie jest zaskoczeniem, że wykonanie pełnej analizy powłamaniowej (o ile w ogóle jest możliwe) jest kwestią miesięcy, jeżeli nie lat. Dla menedżera (lub polityka), który chce pokazać, że podjął szybkie i zdecydowane działania, i który jest przyzwyczajony do szybkiej reakcji i otrzymywania rezultatów na bieżąco, taki czas reakcji jest niemożliwy do zaakceptowania.

Straty wizerunkowe i chaos komunikacyjny

> W miarę rozwoju incydentu hakerzy udostępniali kolejne informacje. Ranga ujawnianych dokumentów była eskalowana w reakcji na próby umniejszania skutków ataku przez decydentów.

Cyberincydenty stanowią bardzo trudne wyzwanie z perspektywy wizerunku ofiar ataku. Nie jest jasne dlaczego, ale ofiary cyberataków (i to zarówno instytucje, jak i osoby pry-

watne) nie spotykają się z empatią ze strony opinii publicznej, mimo że straty, których doświadczają, mogą być większe niż przy innych zdarzeniach. Przy awarii linii produkcyjnej, wypadku czy zdarzenia o charakterze losowym (pożar, powódź) możemy liczyć na zrozumienie dla trudnej sytuacji, w jakiej się znaleźliśmy, i wsparcie ze strony osób trzecich. Typowa reakcja na cyberatak jest zupełnie inna – osoby postronne (często słusznie) postrzegają ofiarę jako współwinną zaistniałej sytuacji. Zarządzając stratami wizerunkowymi, nie możemy liczyć na taryfę ulgową. Rola wyważonej komunikacji przy kryzysie wywołanym cyberatakiem ma dla ochrony wizerunku znaczenie absolutnie kluczowe. W sytuacji, w której incydent w naturalny sposób eskaluje w czasie, a my nie dysponujemy pełną informacją na temat zdarzenia, zadanie to jest dodatkowo utrudnione.

Przy klasycznej awarii sprzętu czy linii produkcyjnej możemy nie być w stanie od razu ocenić długofalowych skutków zdarzenia dla naszego biznesu. Zazwyczaj jednak od początku wiemy, jaki jest charakter czy skala uszkodzeń i strat materialnych. W typowym cyberincydencie skala zdarzenia (włamania, wycieku informacji) odkrywa się nam stopniowo, w miarę jak orientujemy się, że kolejne serwery czy konta kolejnych użytkowników zostały przejęte przez hakerów. Zanim dokonamy analizy zdarzenia (a to wymaga czasu), zazwyczaj nie wiemy, jakie będą kolejne etapy eskalacji incydentu. Decydenci ulegający pokusie obrony swojego wizerunku jako osób mocnych, trzymających sytuację w garści, ale przyzwyczajeni do reagowania na kryzysy innego typu, często zapominają o możliwości eskalacji incydentu.

Słabe programy szkoleniowe dla pracowników

> Jedną z reakcji na incydent w KPRM było przeprowadzenie szkolenia z cyberbezpieczeństwa dla szerszej grupy polityków. Szczegóły szkolenia zostały utajnione, ale w doniesieniach prasowych i komentarzach dominowały opinie, że jego jakość była nie najlepsza.

O tym, że ludzie są najsłabszym ogniwem cyberbezpieczeństwa, słyszymy na każdym kroku. Trudno jest znaleźć dobre szkolenie, które pozwala na podnoszenie kompetencji pracowników w sposób atrakcyjny i skuteczny. Rzadko można osiągnąć dobre rezultaty, oferując pracownikom standardowe szkolenie „z półki", na którym ekspert opowiada o rozwiązaniach niestosowanych w danej instytucji, używając hermetycznego, specjalistycznego żargonu.

Szkolenia z zakresu cyberbezpieczeństwa są bardzo często traktowane (podobnie jak szkolenia BHP) jako nieprzydatny obowiązek. Czasami, dla poprawy ich atrakcyjności, narracja tych szkoleń jest wzbogacona o opis kilku spektakularnych cyberincydentów i koncentruje się na opisywaniu luk systemowych. Takie podejście pogłębia jednak lukę komunikacyjną, zamiast tłumaczyć kwestie cyberbezpieczeństwa w sposób przystępny dla użytkowników.

W temacie cyberbezpieczeństwa brakuje otwartej komunikacji – zachęcania użytkowników do korzystania z pomocy w sytuacji, gdy podejrzewają, że mają do czynienia z cyberatakiem, i tłumaczenia im, jakie praktyczne działania mogą podejmować, aby uniknąć stania się ofiarą cyberincydentu. W tym kontekście próbę utajnienia, że odbyło się szkolenie z cyberbezpieczeństwa, ciężko jest określić inaczej niż jako całkowite nieporozumienie. O dziwo, takie podejście jest zaskakująco często spotykane w praktyce.

Prywatne i służbowe zasoby informatyczne

> U podstaw incydentu leżała praktyka wykorzystania do służbowej korespondencji prywatnych skrzynek mailowych zlokalizowanych na publicznych serwisach sieciowych. Z uwagi na ich prywatny charakter zasoby te nie były objęte ochroną ze strony służb odpowiedzialnych za bezpieczeństwo informatyczne KPRM.

Nagłośnienie incydentu w KPRM na pewno pomogło w zbudowaniu świadomości zagrożeń związanych z łącze-

niem technologii wykorzystywanej do celów prywatnych i służbowych. Wysyłanie służbowych informacji z prywatnej poczty dalece odbiega od zasad „dobrej praktyki" w ochronie informacji i możemy się spodziewać, że jest zabronione w każdej instytucji, która wdrożyła choćby najbardziej podstawowe zasady bezpieczeństwa. Ale sam zakaz nie rozwiązuje znacznie szerszego problemu, który obecnie stanowi jedno z największych wyzwań technologicznych w zakresie ochrony informacji.

Instytucje mogą i powinny przeciwdziałać wykorzystywaniu zasobów prywatnych do celów służbowych lub, alternatywnie, służbowych do celów prywatnych. W praktyce jednak pełne wyeliminowanie tego zjawiska jest niemożliwe. Korzystanie do celów służbowych z rozwiązań nieudostępnianych oficjalnie przez pracodawcę ma charakter powszechny.

Jak pokazuje praktyka, problem (choć w różnej skali) dotyka każdej instytucji. W dobie rozwiązań chmurowych zasobem informatycznym wykorzystywanym przez pracownika nie musi być poczta czy systemy do wymiany plików. Mogą to być programy do graficznej obróbki danych pozwalające na tworzenie atrakcyjnych prezentacji, rozwiązania wspierające pracę grupową czy programy do konwersji zdjęć na tekst, albo programy tłumaczące. Wykorzystanie tych narzędzi nie wynika z intencji działania na szkodę firmy lub z nieznajomości obowiązujących w firmie zasad bezpieczeństwa. Rozwój technologii wykorzystywanych przez te narzędzia postępuje na tyle szybko, że wymykają się one próbom regulacji i znajdują się w szarej strefie między tym, co jest zakazane, i tym, co jest dopuszczone do wykorzystania w danej instytucji.

Przy wszechobecnej technologii trudno podać jednoznaczną receptę, gdzie znajduje się złoty środek i rozsądna granica między służbowym i prywatnym wykorzystaniem zasobów informatycznych. Określenie, jakie nakłady chcemy poświęcić na ograniczenie ryzyka związanego z wyciekiem informacji (lub włamaniem) tym kanałem, to jedna z trud-

niejszych decyzji, która dodatkowo niesie ze sobą poważne skutki finansowe związane z zakupem i utrzymaniem sprzętu i zabezpieczeń. Na pewno z perspektywy instytucji warto rozumieć, jaka jest rzeczywista skala tego zjawiska, i reagować, kiedy przyjmuje niepokojące rozmiary. Rozwiązaniem nie jest administracyjny zakaz korzystania z prywatnych urządzeń lub kont pocztowych i ogłoszenie, że zagrożenie jest wyeliminowane.

> Teoretycznie możemy postawić granicę i domagać się od pracowników korzystania dla celów zawodowych tylko ze służbowego sprzętu, i zablokować możliwość dostępu ze służbowych komputerów do poczty innej niż firmowa. To proste rozwiązanie zaczyna jednak bardzo szybko się komplikować, jeżeli rozważymy przypadek bardziej skomplikowany niż pracownik przychodzący do biura na 8 godzin i niepracujący jednocześnie w innej instytucji. Jakie rozwiązanie przyjąć dla osób pracujących w niepełnym wymiarze czasu? Czy będziemy oczekiwali, że konsultant (z którego usług korzystamy 5 dni w miesiącu i pracujący z 3–4 firmami) otrzyma od nas sprzęt firmowy, czy raczej pozwolimy mu podłączać się do naszej sieci ze swojego sprzętu? A może jednak pozwolimy pracownikom łączyć się do służbowych telekonferencji i poczty firmowej z prywatnego komputera w domu? Jak rozwiązać problem urządzeń mobilnych? Kupujemy je na koszt firmy dla wszystkich pracowników, czy jednak dopuszczamy wykorzystanie urządzeń prywatnych?

Musimy mieć świadomość, że duża część współczesnych pracowników wie, jak wykorzystywać w pracy nowoczesne technologie, i chce to robić. Jeżeli nasza infrastruktura techniczna nie będzie wspierała takich możliwości, to pracownicy będą obchodzili narzucone przez pracodawcę ograniczenia, korzystając z rozwiązań prywatnych dostępnych w domenie publicznej. Zjawisko to otwiera nas na wiele dodatkowych ryzyk z zakresu bezpieczeństwa, ale z drugiej strony, umiejętnie wykorzystane, może być źródłem cennej innowacji.

Poleganie na fachowcach

> Incydent w KPRM był w oczywisty sposób nośny medialnie i szeroko komentowany, ale warto zwrócić uwagę, że komentującymi byli najczęściej sami dziennikarze albo, częściej, eksperci merytoryczni z zakresu bezpieczeństwa informatycznego. Wśród komentujących było stosunkowo niewielu polityków czy menedżerów z doświadczeniem w zarządzaniu instytucjami publicznymi. Sądzę, że gdyby podobnej rangi incydent dotyczył dowolnego innego obszaru działalności KPRM (finansów, organizacji, nadzoru nad funduszami unijnymi), to pokusa do skomentowania wydarzeń byłaby z ich strony znacznie silniejsza.

Brak komentarzy dotyczących incydentu w KPRM ze strony doświadczonych menedżerów znakomicie ilustruje stosunek kadry menedżerskiej do tematu cyberbezpieczeństwa. Autorzy publikacji w mediach stale podnoszą znaczenie zagrożenia związanego z cyberbezpieczeństwem i stale postulują, że tematyka ta powinna być przedmiotem zainteresowania i nadzoru ze strony zarządzających. Eksperci zalecają, żeby okresowo (co pół roku lub co kwartał) temat cyberbezpieczeństwa był omawiany na posiedzeniach zarządów i rad nadzorczych, podobnie jak omawiane są inne kwestie związane z zarządzaniem. Praktyka pokazuje, że sytuacja wygląda zupełnie inaczej. Temat jest delegowany w pełnym zakresie do „fachowców", a kadra zarządzająca omawia go najczęściej dopiero wtedy, gdy jest to absolutnie konieczne.

O ile w instytucjach, które nie zostały jeszcze dotknięte skutkami działalności cyberprzestępców, taki stan rzeczy może wydawać się zrozumiały, o tyle – jak widzimy – zjawisko to występuje także wśród ofiar poważnych cyberataków. Analizując reakcje na cyberincydenty, bardzo często ze strony kadry menedżerskiej spotykamy się z komunikatem: „jesteśmy ofiarą przestępstwa i przekazaliśmy incydent do zbadania odpowiednim służbom". W ocenie zarówno samych

zarządzających, jak i bardzo często w ocenie opinii publicznej takie postawienie sprawy jest wystarczające.

W instytucji, która nie dysponuje środkami pozwalającymi na samodzielne techniczne zbadanie incydentu, zaangażowanie ekspertów do analizy incydentu jest jak najbardziej uzasadnione. Ale nawet jeżeli mamy takie możliwości, wymiana doświadczeń z innymi może pozwolić na lepsze zrozumienie charakteru zdarzenia i skorzystanie ze sprawdzonych rozwiązań w wypracowywaniu reakcji na incydent. Udział ekspertów sam w sobie nie jest problemem, natomiast zakres, w jakim menedżerowie polegają na ekspertach – oddając w ich ręce całość decyzji w zakresie cyberbezpieczeństwa – jest zupełnie wyjątkowy w porównaniu do innych obszarów zarządzania.

> Przez analogię: firmy często angażują doradców do przedstawiania propozycji produktów inwestycyjnych poprawiających zarządzanie finansami firmy, ale raczej nie zdarza się, aby rada nadzorcza zaakceptowała sytuację, w której dyrektor finansowy całkowicie zdelegował zarządzanie finansami na bank, albo nie oczekiwała od niego raportów na temat kondycji finansowej.

Przyczyna takiej sytuacji jest głębsza. To nie tylko chęć (czy próba) pragmatycznego przeniesienia odpowiedzialności za trudny technicznie obszar na kogoś innego. U jej podstaw leży przekonanie, że możliwości bezpośredniego wpływu kadry menedżerskiej na stan cyberbezpieczeństwa są stosunkowo niewielkie, gdyż nadzorowanie tego obszaru wymaga specjalistycznej wiedzy technicznej. Postawa samych ekspertów (którzy w naturalny sposób są zainteresowani, aby nie być przedmiotem nadmiernej uwagi ze strony zarządzających) także nie służy przełamaniu tej bariery. Typowa narracja ze strony ekspertów zazwyczaj koncentruje się na technicznych zagadnieniach zrozumiałych tylko dla fachowców, a zarządzający utwierdzają się w przekonaniu, że ich udział w dyskusji na temat cyberbezpieczeństwa nie jest konieczny i niewiele wnosi.

Na rynku bardzo rzadko mamy do czynienia z sytuacją, w której ekspert jest w stanie pokazać związek między technologią, bezpieczeństwem i celami biznesowymi danej instytucji, dzięki czemu zarządzający są w stanie aktywnie uczestniczyć w formułowaniu strategii bezpiecznego wykorzystania nowoczesnych technologii do wspierania nowych pomysłów biznesowych i innowacji.

> Niniejsza książka jest próbą sprostania temu wyzwaniu i przygotowania menedżerów do udziału w takiej dyskusji z ekspertami. Ambicją autora jest, aby z jednej strony przystępnie wytłumaczyć podstawowe pojęcia z zakresu bezpieczeństwa informatycznego czytelnikom, którzy nie dysponują wiedzą techniczną, z drugiej zaś strony pokazać i zilustrować przykładami sytuacje, w których związek między cyberbezpieczeństwem a działalnością instytucji jest na tyle istotny, że powinien stanowić obszar szczególnej uwagi ze strony zarządzających.

Cyberatak to dzisiaj jedno z poważniejszych zagrożeń dla biznesu, a przygotowanie firmy na atak hakerów, który nieuchronnie nastąpi, to jedno z największych wyzwań dla kadry zarządzającej.

Jakub Bojanowski od ponad 20 lat pomaga firmom chronić się przed cyberatakami, a swoje doświadczenie z zakresu bezpieczeństwa informatycznego zdobywał w międzynarodowej firmie doradczej. Pisząc tę książkę, chciał pokazać, w jaki sposób kadra menedżerska powinna uczestniczyć w zarządzaniu bezpieczeństwem, i udowodnić, że temat cyberbezpieczeństwa wcale nie jest tak skomplikowany, jak się powszechnie uważa. Jeśli więc chcesz zrozumieć, na jakie cyberzagrożenia musimy być przygotowani, to w *Zdążyć przed hakerem* znajdziesz wyjaśnienia najważniejszych zagadnień technicznych – zilustrowane *case studies* i przykładami z bogatej praktyki zawodowej autora. Ta wiedza pozwoli każdemu menedżerowi, nawet z bardzo podstawową znajomością informatyki, odegrać ważną rolę w tworzeniu firmowego programu cyberbezpieczeństwa i podejmować dialog z ekspertami.

Po przeczytaniu tej książki:

- Dowiesz się, w jaki sposób hakerzy wybierają swoje ofiary, jak działają i jaką mają motywację.
- Zidentyfikujesz zasoby informatyczne firmy, które są szczególnie narażone na cyberzagrożenia.
- Poznasz standardy i kanony dobrej praktyki w zarządzaniu bezpieczeństwem informacji.
- Dowiesz się, jak kadra menedżerska powinna współpracować z fachowcami technicznymi i specjalistami od bezpieczeństwa, aby wspierać rozwój biznesu.
- Zrozumiesz, w jaki sposób i dlaczego pieniądz elektroniczny i systemy płatności on-line są narażone na ataki hakerów i dlaczego stosowane w tym obszarze zabezpieczenia i technologie muszą być cały czas rozwijane.
- Poznasz działania, które należy podejmować, aby ataki hakerów wykrywać odpowiednio wcześnie i ograniczać ich negatywne skutki.
- Dowiesz się, jak postępować, aby w sytuacji, kiedy firma jest ofiarą cyberataku, swoimi działaniami nie pogłębiać kryzysu i zachować swój wizerunek sprawnego i kompetentnego menedżera, który jest w stanie sprostać nawet tak trudnemu wyzwaniu.

Patronat:

MY COMPANY POLSKA | THINKTANK | HR personel & zarządzanie | NOWA SPRZEDAŻ

www.mtbiznes.pl Książka dostępna również jako e-book

ISBN 978-83-8231-197-6

9 788382 311976

MT 22036
Cena 64,90 zł