Strażnicy niefortunnych słów

Jeden nieprzemyślany e-mail szeregowego pracownika może kosztować firmę miliony. Co poradzić? Kontrolować korporacyjne e-maile? Syzyfowe prace. Edukować pracowników? Nie wystarczy. A może zdać się na speców od IT i ich programy filtrujące?

Korupcję znam z gazet, o zmowie cenowej słyszałem w telewizyjnych reklamach. Nieuczciwa konkurencja? Zawsze gram fair! Nie ma więc szans, by UOKiK czy CBA zainteresowały się moją firmą – tak myśli zapewne większość przedsiębiorców, którzy nie są na bakier z etyką i prawem. Czy tacy biznesmeni rzeczywiście mogą spać spokojnie?

– Niezupełnie – odpowiada **dr Marcin Matczak** ze znanej kancelarii prawniczej Domański Zakrzewski Palinka. I dodaje: – Podejście do stosowania prawa w ostatniej dekadzie bardzo się zmieniło. Teraz urzędy państwowe skupiają się coraz bardziej na badaniu szerokiego kontekstu funkcjonowania firmy, a nie tylko pojedynczym, konkretnym działaniu. W największym skrócie: firmy coraz częściej odpowiadają za dane działania nie dlatego, że są one same w sobie są nielegalne, ale dlatego, że ich kontekst wskazuje na niezgodne z prawem intencje ich dokonywania.

Rzeczywiście, zdarzają się wyroki „za zamiar". A zdarzają się i wyroki... za nieporozumienie.

Niepozorne ryzyko

– Nie tylko prokuratura, ale także UOKiK, np. w decyzjach dotyczących zakazanych porozumień antykonkurencyjnych, nierzadko uprawdopodabniają istnienie takiej umowy, cytując e-maile zdobyte w czasie kontroli. Bez dowodów w postaci e-maili nałożenie kar w takich przypadkach często nie byłoby możliwe – wyjaśnia Marcin Matczak. Tyle teorii. Może jakiś konkret? – Załóżmy, że firma farmaceutyczna organizuje zagraniczny wyjazd dla lekarzy. Cel: zapoznanie ich z lekiem, opis jego działania, odpowiedzi na pytania. To legalne. A teraz, załóżmy, że przedstawiciel uzasadnia w e-mailu do przełożonego, że celem wysłania konkretnego lekarza na taki wyjazd jest skłonienie go do „przepisania w następnym miesiącu o 25 proc. więcej opakowań leków firmy". I to już może być nielegalne. Nawet jeśli ów e-mail jest „skrótem myślowym", firma może mieć ogromne problemy – wskazuje prawnik.

E-mailowy ciąg dowodów to nie sytuacja hipotetyczna. W zeszłym roku udowodniono chociażby zmowę cenową firmie Polifarb i sieci marketów Leroy Merlin. Każdą z firm ukarano 32 mln zł. Do takiej, a nie innej sentencji wyroku przyczyniły się zapiski w notatkach i e-mailach. Zresztą, UOKiK specjalnie nie ukrywa, że treść e-maili prowadzi często do wyroków. „Bywa, że nie znajdujemy dokumentów potwierdzających zmowę. Ale zwykle coś jest... Jakieś pismo, zapiski" – opowiadała **Katarzyna Róziewicz** w „Polityce". Zdaniem dr. Matczaka, nie tylko obawa przed polskimi służbami motywuje szefów rodzimych firm do zajęcia się sprawą bezpieczeństwa e-maili. – Granice mają coraz mniejsze znaczenie dla służb antymonopolowych. A i dla biznesu nie liczą się już od dawna. Nietrudno więc sobie wyobrazić, że amerykańskie urzędy interesują się firmami z centralnej Europy. Takie sytuacje wielokrotnie już się zdarzały – wskazuje Marcin Matczak.

↑ Andrzej Geryk, ForCompany

Środek ochronny

Jak się ochronić przed lekkomyślnymi e-mailami pracowników? Kasować je? – Nawet jeśli codziennie, pod koniec dnia, kasowalibyśmy e-maile, to przecież zostały one gdzieś wysłane. A nad odbiorcami wiadomości kontroli nie mamy i nie będziemy mieć, poza tym chodzi o prewencję, a nie o maskowanie naruszeń prawa – wskazuje **Andrzej Geryk** z firmy ForCompany. I proponuje rozwiązanie: program Sentinel, przygotowany zresztą we współpracy z prawnikami z kancelarii Domański Zakrzewski Palinka.

System ten ma wychwytywać zbitki i frazy mogące sugerować intencję naruszenia prawa przez pracowników firmy. – Taki program przyda się firmie niezależnie od branży, w jakiej pracuje. Choć niewątpliwie największe zainteresowanie Sentinel budzi w branży farmaceutycznej – wyjaśnia Andrzej Geryk.

Autorzy nie ukrywają, że tworząc Sentinela inspirowali się pomysłami zza Atlantyku, gdzie służby śledcze i antymonopolowe działają wyjątkowo sprawnie. – Nasz program dostosowaliśmy jednak do polskich realiów, a prawnicy na bieżąco go aktualizują – dopowiada Andrzej Geryk. Prezes firmy po zakupie Sentinela dostaje raporty, który pracownik w e-mailach używa niebezpiecznych fraz i dzięki temu może podjąć działania prewencyjne, nie dopuszczając do naruszenia prawa. Andrzej Geryk podkreśla, że dzięki współpracy z kancelarią program wychwytuje niezręczne sformułowania zaraz po nowelizacji prawa, która doprowadziła do możliwej, kłopotliwej interpretacji treści e-maila.

A co przedstawiciele branży informatycznej mają do powiedzenia o Sentinelu? – Mechanizm działania programu przypomina tzw. Bayesian Filter – opartą na statystyce technikę filtrowania treści e-maili. Filtry tego typu – mimo iż nie należą do najnowszych – nadal są dość efektywne w kontroli zawartości wiadomości

elektronicznych – ocenia **Roger Thompson,** Chief Research Officer w AVG Technologies.

– Działanie Sentinela opiera się głównie na połączeniu unikalnej dla języka polskiego analizy językowej, uwzględniającej synonimy czy gramatykę, z najnowszymi metodami sztucznej inteligencji, uczenia maszynowego i analizy statystycznej. To rozwiązania wykraczające poza proste kontekstowe wychwytywanie słów kluczowych, wyznaczające najnowsze trendy w filtrowaniu komunikacji. – uważa Andrzej Geryk.

Przyczajone niebezpieczeństwa

Sentinel nie jest bynajmniej jedyną tego typu propozycją na polskim rynku. – Juniper Networks i SurfControl oferują rozwiązanie zapewniające wielowarstwowe wykrywanie i kontrolowanie zagrożeń – i istniejących, i tych, które dopiero powstają. SurfControl Web Filter, zintegrowany z rozwiązaniami Juniper Networks, umożliwia filtrowanie według reguł globalnych lub specyficznych dla użytkownika, z uwzględnieniem kategorii, treści, typu pliku – opowiada **Wojciech Głażewski,** Country Manager Juniper Networks. I dorzuca: – Najprościej, gdyby pracownicy podchodzili z większą rozwagą do przesyłanych treści. Ale firmy nie mogą pozwolić sobie na takie „życzeniowe myślenie". Dlatego stosują rozwiązania, które zgodnie z wewnętrznymi politykami pozwalają automatycznie i inteligentnie zarządzać zagrożeniami ukrytymi w e-mailach.

Własne rozwiązania poleca też np. Symantec. – Oferujemy Symantec Data Loss Prevention, które używa algorytmów rozpoznawania treści właśnie w celu ochrony przed wyciekiem danych – mówi **Piotr Chrobot,** dyrektor zarządzający w Symantec Polska.

– E-maile są i będą podstawowym środkiem komunikacji w przedsiębiorstwach. I można je nieźle chronić. Ale Internet i zwyczaje pracowników korporacji zmieniają się szybko. Dostęp do Internetu oferuje wiele sposobów, by rozpowszechniać niewygodne dla firm informacje – wystarczy wspomnieć o możliwościach portali społecznościowych – zauważa Roger Thompson.

No, to co: czekać na programy, które i w przypadku takich portali ochronią nasze dane? A może jednak lepiej edukować pracowników? I tu wracamy do punktu wyjścia. ⇤

Mateusz Madejski

E-maile: Pfizer pod pręgierzem

W ramach ugody farmaceutyczny gigant, Pfizer, zgodził się zapłacić 2,3 mld dol. amerykańskim władzom federalnym. Były pracownik Pfizera, John Kopchinski, w 2003 r. pozwał firmę, zarzucając jej nielegalne praktyki w reklamie leku przeciwbólowego Bextra. Zarzuty poparł dokumentami, do których miał dostęp jako przedstawiciel handlowy Pfizera (większość to e-maile). W jednym z elektronicznych listów kierownik działu kończy wiadomość do handlowca stwierdzeniem: „Świetna robota, 5000 punktów w drodze". Dzięki innym materiałom udało się udowodnić, że punkty te były zapłatą za nielegalne praktyki i że wymieniano je na pieniądze. Elektronicznie przekazywane wieści pozwoliły też udowodnić, że Pfizer powszechnie praktykował wynagradzanie lekarzy za uczestnictwo w „spotkaniach promocyjnych leku Bextra".

Fot. ARC