



Tomasz Furman
tomasz.furman@parkiet.com



Martyna Izdebska-Tran
martyna.izdebska-tran@parkiet.com



Urządzenie podsłuchowe z możliwością nagrywania (1), urządzenie podsłuchowe zamontowane w długopisie (2) oraz breloku (3) i mikrokamera z dyktafonem (4). FOT. W. WASYLUK

Szpiegostwo gospodarcze jest coraz powszechniejsze

W ocenie specjalistów dostęp do poufnych informacji firm próbuje uzyskać coraz więcej nieuprawnionych osób. Z drugiej strony systemy zabezpieczeń są dalece niewystarczające, z czego nie wszystkie spółki zdają sobie sprawę

Z każdym rokiem szpiegostwo przemysłowe, rozumiane jako kradzież tajemnic handlowych, własności intelektualnej czy danych klientów, przybiera na sile. Doświadczają go zwłaszcza nie tylko międzynarodowe koncerny, takie jak Coca-Cola Company, której pracownik próbował sprzedać tajne informacje najgroźniejszemu konkurentowi - firmie PepsiCo. Coraz częściej z podobnymi problemami borykają się polskie spółki. Wystarczy przypomnieć skandal, który jesienią wybuchł w giełdowej grupie energetycznej Enea. Jej związkowcy oskarżyli firmę TFS o szpiegostwo gospodarcze, gdy ta, badając systemy zabezpieczeń w Enei, zażądała wglądu w jej umowy handlowe.

Leczenie skutków
W ocenie specjalistów niewiele spraw dotyczących kradzieży informacji stanowiących tajemnice firm wychodzi na jaw, mimo że takich sytuacji jest coraz więcej. - Szpiegostwo przemysłowe w Polsce jest obecnie zjawiskiem powszechnym. Niestety, spółki raczej próbują leczyć skutki wpływu ich tajemnic, niż zapobiegać temu procederowi - mówi Michał Rapacki, prezes Business Security Agency, biura detektywistycznego oferującego usługi w zakresie bezpieczeństwa biznesu.

- Jedną z najbardziej zagrożonych jest branża farmaceutyczna. Zaraz za nią są nowe technologie, ale tak naprawdę wszędzie tam, gdzie są duże pieniądze i ostra walka o rynek, o kontrakty, będziemy mieli do czynienia ze zjawiskiem szpiegostwa gospodarczego - twierdzi Artur Frydrych, specjalista bezpieczeństwa biznesu JDS Consulting.

Podsłuchy i mikrokamery
W powszechnym odbiorze szpiegostwo gospodarcze wiąże się ze stosowaniem podsłuchów i mikrokamer, dzięki którym niepowołane osoby i instytucje mogą usłyszeć i zobaczyć to, czego wiele firm wolałoby nie ujawniać. Dzieje się tak, chociaż część stosowanych urządzeń powinna być dostępna tylko dla ustawowo upoważnionych instytucji, takich jak policja, wojsko czy służby specjalne. Z drugiej jednak strony ich nabycie nie jest specjalnie utrudnione. Każdy chętny przed zakupem podsłuchów lub mikrokamer musi jedynie podpisać oświadczenie, w którym m.in. stwierdzi, że nie użyje ich na terenie Unii Europejskiej. To z kolei zmusza spółki do działań prewencyjnych. - Gdy mieliśmy podejrzenie, że ktoś nas podsłuchuje, wynajęliśmy specjalistyczną firmę, która przeszukała nasze pomieszczenia pod kątem obecności niepożądanych urządzeń. Polegało ono m.in. na elektronicznym i fizycznym sprawdzeniu miejsc, w których można założyć podsłuch - przyznaje Maciej Radziwiłł, prezes

Trakcji Polskiej. Nadajników można też poszukiwać samemu. Zakup miernika częstotliwości, który to umożliwia, kosztuje około 900 zł.

Problemy z zagłuszcaczami
Na rynku dostępne są też zagłuszcacze podsłuchów. Ich cena waha się od 2 do 4 tys. zł. Z nimi wiąże się jednak pewne zagrożenie. - Gdy przeprowadzono ważne i poufne spotkanie, firma stosowała urządzenia zagłuszające, które dodatkowo uniemożliwiały prowadzenie jakiegokolwiek rozmów przez telefon komórkowy w promieniu kilkudziesięciu metrów. Wówczas niektórzy pracownicy, aby połączyć się telefonicznie z inną osobą, musieli wychodzić na zewnątrz budynku - mówi jeden z byłych dyrektorów Polskiego Górnictwa Naftowego i Gazownictwa. Dodaje, że w spółce są specjalne pomieszczenia przeznaczone do prowadzenia poufnych rozmów handlowych, posiadanych przez zarząd, spotkania dotyczących budżetu i innych o istotnym znaczeniu dla działalności grupy. - Na pozór takie pomieszczenia niczym się nie różnią od zwykłych gabinetów niedostępnych dla ludzkiego oka miejscach znajdujących się jednak urządzeniami uniemożliwiającymi podsłuch czy podgląd tego, co się dzieje w środku - dodaje były dyrektor PGNiG.

Firmy sprawdzają też gabinety i sale konferencyjne, poszukując podsłuchów tuż przed spotkaniem, w czasie

których będą prowadzone ważne rozmowy. - Jednocześnie nie biorą pod uwagę, że podsłuch może być nieświadomie wniesiony do sprawdzonego pomieszczenia przez uczestnika zebrania. Takie zabezpieczenie, bez dalszych procedur bezpieczeństwa, to zmarnowane pieniądze - przestrzega Frydrych.

Grożne gadżety
Asortyment urządzeń, które mogą być wykorzystane do kradzieży poufnych informacji, systematycznie rośnie i stanowią coraz większe zagrożenie. Słabym ogniwem w wielu firmach są systemy informatyczne. Dziś nie wystarczy już programy antywirusowe, antywlamanio-we, antyspamowe, hasła do komputera czy nawet poszczególnych plików. Wiele firm oferuje urządzenia USB, które omijają te zabezpieczenia i rejestrują zrzuty ekranu, znaki wpisane na klawiaturze komputera, odwiedzane strony w sieci i rozmowy w komunikatorach tekstowych (np. Gadu-Gadu). Zagrożenie stwarzają technologie tempostowe, które pozwalają nieuprawnionym osobom (za pośrednictwem czulego odbiornika) przechwytywać obraz z wia-

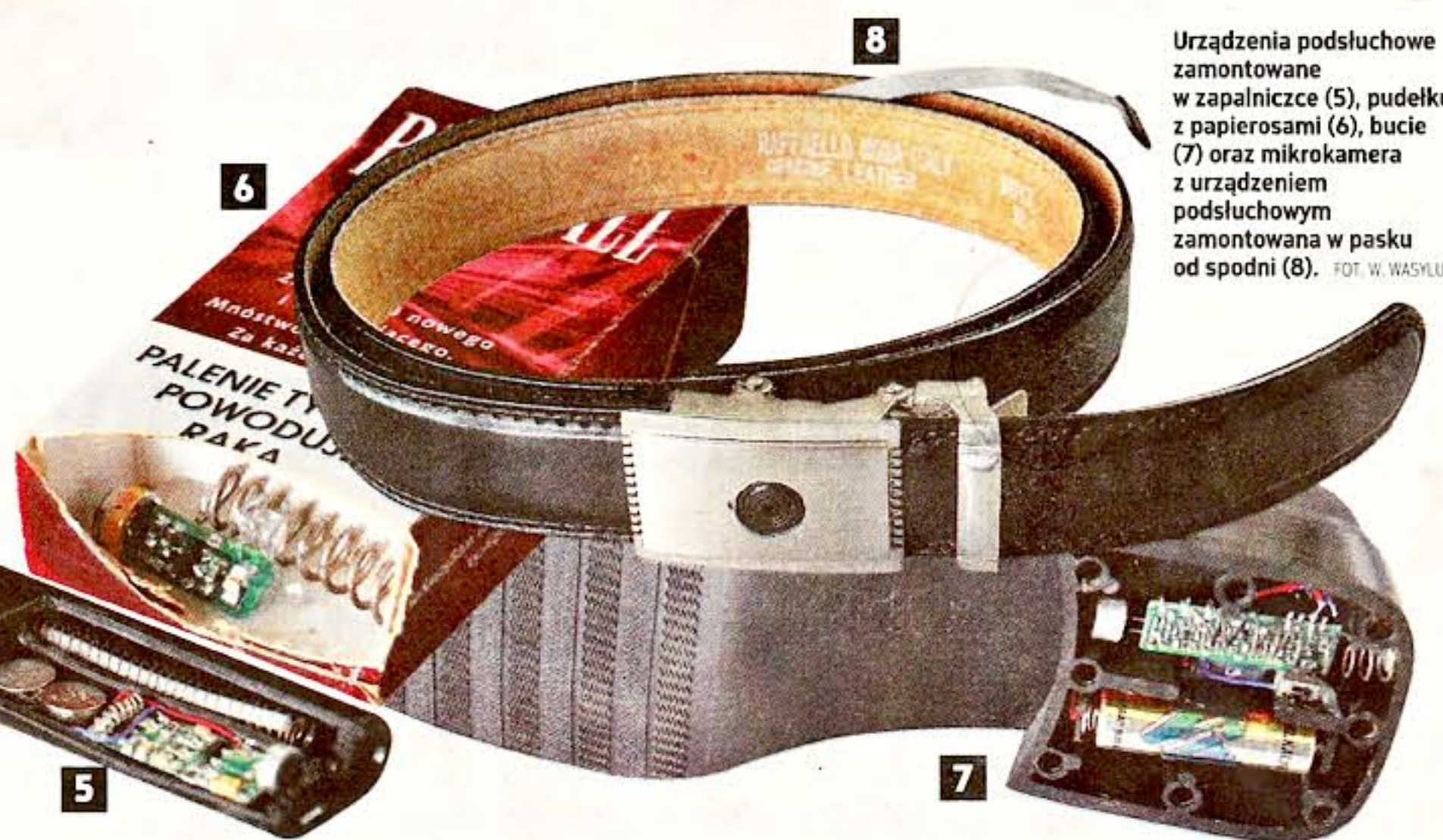
nych w danej firmie. Jednak większość poufnych informacji wydostaje się na zewnątrz nie dzięki zainstalowanym urządzeniom szpiegowskim, lecz ludziom. Eksperti są zgodni, że nieodpowiednio zabezpieczone systemy komputerowe to tylko około 10 proc. zagrożenia. - Ponad 80 proc. wycieków następuje przez osoby, które mają bezpośredni dostęp do danych - mówi Rapacki. Dodaje, że może do tego dochodzić wskutek przełupstwa, przejęcia korespondencji, a nawet przez zatrudnienie „swojego szpiega” w firmie, którą interesuje się konkurencja.

Informacje poufne
Ogół firm giełdowych prawdopodobnie największą uwagę

zwraca na ochronę tajemnicy zawodowej i informacji poufnych ściśle zdefiniowanych w prawie o publicznym obrocie papierami wartościowymi. Powodem są sankcje pieniężne, a nawet karne, które się wiążą z ich ujawnieniem lub wykorzystaniem. Dla przykładu, kto wbrew zakazowi wykorzystuje informację poufną, podlega grzywnie do 5 mln zł albo karze pozbawienia wolności od trzech miesięcy do lat pięciu albo obu tym karom łącznie. Najczęściej są to dane mające wpływ na notowania papierów wartościowych spółek z GPW. Jak się zabezpieczyć przed ich wyciekiem? - Liczba osób mających dostęp do informacji poufnych musi być jak najmniejsza, a także, jeżeli to możliwe, ostateczna wersja informacji powinna powstawać jak najpóźniej. Należy również zadbać, aby dostęp do nich miały jedynie osoby sprawdzone - mówi Radziwiłł. Dodaje, że jeśli chodzi o jego spółkę, największe znaczenie mają informacje o składanych ofertach w przetargach na mo-

szanych przez PKP PLK. Chodzi zwłaszcza o cenę, która zazwyczaj jest kryterium decydującym o wyborze zwycięzcy. Przy przetargach powszechnym bledem jest jednak zapominanie, że każda informacja ma swoją kopię. - Firmy, dbając o utrzymanie w największej tajemnicy treści składanej oferty lub zawartej umowy, dokładają ogromnych starań, aby te informacje nie wyciekły na zewnątrz. Jednocześnie ich część często konsultują z zewnętrzną kancelarią prawną, nie zastanawiając się w ogóle nad tym, że tam ten dokument jest chroniony bardzo słabo - ostrzega Frydrych.

Kancelarie tajne
Kolejnym sposobem, który ma zapobiegać wydostaniu się



Wszędzie tam, gdzie są duże pieniądze i ostra walka o rynek oraz kontrakty, mamy do czynienia ze zjawiskiem szpiegostwa gospodarczego i próbami zabezpieczania się firm przed wpływem poufnych informacji.

ochrony informacji niejawnych. W sumie to kilkadziesiąt osób - informuje biuro prasowe Grupy Lotos. Kancelarie tajne mają również filmy budowlane, informatyczne i inne, które wykonują określone prace w celu zapewnienia dostępu do ważnych z biznesowego punktu widzenia dokumentów. Przedstawiciele zarządu Enei stwierdzili, że działania te były konieczne, by sprawdzić, kto ma dostęp do ważnych dokumentów. Związkowcy jednak zakwestionowali czytelność działań TFS. Pojawiły się plotki, że spółka doradczą wyprodukuje z firmy dane, które może wykorzystać jeden z zachodnich koncernów zainteresowanych prywatyzacją Enei. Na wynik dochodzenia ABW w tej sprawie trzeba poczekać. Za to w ocenie władz Enei oraz przedstawicieli Ministerstwa Skarbu Państwa powstające spekulacje są celowo nagłaśnianie, choć nie mają żadnych podstaw merytorycznych.

Audyt bezpieczeństwa
Wielu specjalistów uważa, że przed wpływem poufnych informacji, zwłaszcza w firmach, które doświadczyły już takich sytuacji, może uchronić przeprowadzenie audytu bezpieczeństwa. Jego głównym celem jest m.in. ocena stanu bezpieczeństwa w badanym podmiocie. - Prowadzimy takie audyty i tworzymy raporty pokontrolne uwzględniające m.in. konkretne zalecenia dla firm. Prawidłowo wykonany audyt bezpieczeństwa wymaga odpowiedniego sprzętu, wiedzy oraz doświadczenia - mówi Czesław Wiencis, porucznik w stanie spoczynku, prezes Euro-Soft

Poland. Taki audyt powinna przeprowadzić firma zewnętrzna, która może krytycznie spojrzeć na funkcjonujące w danym przedsiębiorstwie procedury i systemy zabezpieczeń. - Zalecenia powinny być wypracowane w sposób niezależny podmiot. Wprowadzone w firmach procedury bezpieczeństwa powinny być na bieżąco sprawdzane, weryfikowane i dostosowywane do aktualnych modeli biznesowych - wyjaśnia Paweł Kozyra, szef komunikacji giełdowego Comarchu.

Przypadek Enei
Dopuszczając inny podmiot do przeprowadzenia audytu bezpieczeństwa, należy jednak zachować szczególną ostrożność, gdyż i w takim przypadku może się okazać, że zaistniało zagrożenie szpiegostwem gospodarczym. Doświadczyla tego grupa energetyczna Enea. Podejrznie szpiegostwa gospodarczego zgłoszono nie tylko do prokuratury, ale też do ABW. Sprawa

zaczęła się kilka miesięcy temu. Obecny prezes Enei Maciej Owczarek po objęciu stanowiska postanowił przeprowadzić audyt bezpieczeństwa obiegu informacji. Zlecenie na wykonanie tego zadania dostała firma i r.o., która uzyskała dostęp do ważnych z biznesowego punktu widzenia dokumentów. Przedstawiciele zarządu Enei stwierdzili, że działania te były konieczne, by sprawdzić, kto ma dostęp do ważnych dokumentów. Związkowcy jednak zakwestionowali czytelność działań TFS. Pojawiły się plotki, że spółka doradczą wyprodukuje z firmy dane, które może wykorzystać jeden z zachodnich koncernów zainteresowanych prywatyzacją Enei. Na wynik dochodzenia ABW w tej sprawie trzeba poczekać. Za to w ocenie władz Enei oraz przedstawicieli Ministerstwa Skarbu Państwa powstające spekulacje są celowo nagłaśnianie, choć nie mają żadnych podstaw merytorycznych.

opinia

Michał Rapacki

PREZES BUSINESS SECURITY AGENCY

Rośnie popyt na usługi wykrywania podsłuchów



Zapotrzebowanie na usługi wykrywania urządzeń podsłuchowych jest coraz większe. Obecnie dostępne są technologie, które pozwalają wykryć nie tylko urządzenia aktywne (nadają sygnał ciągły), ale także pasywne, np. dyktafon lub podsłuchujący nadające pakiet informacji do odbiorcy tylko raz na dobę. Bezprzewodowe urządzenia podsłuchowe mimo niewielkich rozmiarów uzyskują dobry zasięg i jakość dźwięku, jednak jedna bateria zasila je około 14 dni. Niektóre można wpiąć w sieć telefoniczną i mieć zasilanie aż do ich wykrycia. Konkurencja często stosuje urządzenia podsłuchowe w zakresie pozyskania strategicznych informacji o danej spółce. Koszt sprawdzenia, czy w danym pomieszczeniu nie ma takich urządzeń, wynosi od 30 do 50 zł za metr kwadratowy przeszukiwanej powierzchni podłogi. Takie usługi firma zlecająca może wliczyć w koszty. Wojsko czy policja korzystają często z gorszego sprzętu niż oferowany na rynku, chyba że są to wyspecjalizowane służby, np. ABW, CBA czy CBŚ. Te ostatnie użytkują m.in. urządzenia umożliwiające zdalne podsłuchiwanie telefonu komórkowego, do czego zwykły użytkownik nie ma bezpośredniego dostępu. Oczywiście możemy dać komuś telefon z odpowiednim oprogramowaniem do podsłuchiwania rozmów i otoczenia, ale jest to trudniejsze w realizacji i nielegalne. Sprzętu podsłuchowego nie wliczymy też w koszty.

CENY URZĄDZEŃ I USŁUG ZWIĄZANYCH ZE SZPIEGOSTWEM GOSPODARCZYM I OCHRONĄ INFORMACJI POUFNYCH

NAZWA	OPIS	CENA (ZŁ)
Pluskwa	Mikronadajnik do podsłuchu może być wbudowany w gniazdko sieciowe, przedłużacz, kalkulator, zegarek. W zestawie z odbiornikiem.	280-1400
Mikrokamera	Kamera może być wmontowana w krawat, długopis, okulary, guzik.	160-3000
Szpieg tekstu	Urządzenie USB, które rejestruje zrzuty ekranu, znaki wpisane na klawiaturze komputera, odwiedzane strony w sieci i rozmowy w komunikatorach tekstowych (np. gadu-gadu)	160-750
Spyphone	Nokia wraz z zestawem do podsłuchu rozmów, otoczenia, podglądu sms-ów i ustalenia dokładnej lokalizacji GPS	990-4500
Wykrywacz podsłuchu	Zestaw pozwalający na wykrycie urządzeń aktywnych (nadających ciągłe) i nieaktywnych (np. dyktafony lub urządzenia wysyłające pakiet informacji do odbiorcy raz na dobę)	270-4500
Zagłuszcacz podsłuchu	Emuluje dźwięki, które uniemożliwiają odтворzenie głosu z podsłuchu	2000-4000
Usługa wykrywania podsłuchów	Sprawdzanie pomieszczeń na obecność urządzeń podsłuchowych, cena za metr kwadratowy badanej powierzchni	30-50
Programy antywirusowe dla firm	Licencja udzielana na rok (np. Kaspersky, Nod32), cena za jedno stanowisko	70-100
Szkolenia otwarte	Trzydniowe szkolenia otwarte dla pracowników firm, pracowników kancelarii tajnych, w zakresie bezpieczeństwa informacji	3000-4000
Szkolenia zamknięte dla firm	Jeden dzień szkolenia przygotowanego dla konkretnej firmy (dla grupy 30 osób)	od 5000

Źródło: TAYLOR NELSON SORFLEX