Bezpieczna cyberprzestrzeń

Metody działania cyberprzestępców stale ewoluują i niestety wyprzedzają środki obrony przed nieuprawnionymi i nielegalnymi działaniami. W ich wyniku w 2014 r. gospodarka światowa straciła prawie 300 mld dolarów.

Urszula Kamińska

W styczniu br. Akademia Finansów i Biznesu Vistula gościła uczestników zorganizowanej przez Polski Instytut Kontroli Wewnętrznej i ACFE Polska konferencji poświęconej bezpiecznemu wykorzystywaniu cyberprzestrzeni w obrocie gospodarczym. Przedstawiciele ogospodarzy: dr, prof. nadzw. AFiB Vistula Roman Fulneczek oraz Ireneusz Jabłoński, członek zarządu Polskiego Instytutu Kontroli Wewnętrznej, w swoich wystąpieniach podkreślili wagę i konieczność profesjonalnej edukacji oraz potrzebę permanentnego kontaktu i wymiany doświadczeń profesjonalistów odpowiedzialnych za bezpieczeństwo cybernetyczne różnego rodzaju organizacji.

Radosław Chinalski – przedstawiciel firmy Integracja Wiedzy – omówił krajowe i międzynarodowe strategie bezpieczeństwa cybernetycznego. Wskazał najważniejsze elementy rozwiązań służących budowie systemów ochrony cyberprzestrzeni w Polsce i Unii Europejskiej oraz źródła regulacji penalizujących wybrane kategorie czynów zabronionych popełnianych w cyberprzestrzeni. Polską strategię i politykę cyberbezpieczeństwa przedstawił w kontekście strategii bezpieczeństwa narodowego RP. Omawiając Doktrynę Cyberbezpieczeństwa RP, podkreślił wagę działań sektora obywatelskiego, szczególnie stowarzyszenia Polska Obywatelska

Cyberobrona. W podsumowaniu wystąpienia stwierdził, że świadomość zagrożeń w cyberprzestrzeni rośnie zarówno wśród jej indywidualnych jak i korporacyjnych użytkowników. a specjalistyczna edukacja i spotkania takie, jak ta konferencja będą przyczyniać się do poprawy cyberbezpieczeństwa.

W trakcie sesji pytań i odpowiedzi obecna na konferencji Małgorzata Humel-Maciewiczak, Radca Prezesa NIK, powiedziała, że tak istotne dla kraju działania jak budowa bezpieczeństwa cybernetycznego z zasady nie mogą podlegać jednorazowej kontroli NIK i zapewniła, że obywatele mogą być spokojni, iż budowa systemu cyberbezpieczeństwa w Polsce nie pozostanie bez nadzoru i kontroli.

O tym, jak ważne jest stałe monitorowanie systemów informatycznych i nadzorowanie działań poszczególnych ich użytkowników mówił kolejny prelegent – Piotr Błaszczeć, ekspert PIKW, biegły sądowy z zakresu przestępstw przy użyciu sprzętu i sieci komputerowych, audytor systemów IT. Na przykładach z własnej audytorskiej praktyki pokazał typowe błędy i niezgodności z zakresu badania systemów IT, które nie pozwalają na ustalenie osób odpowiedzialnych za powstałe szkody.

Przedstawiciel ComCERT, Dariusz Łydziński opowiedział uczestnikom konferencji, jak zaplanować i wdrożyć dobre praktyki zapobiegania nadużyciom teleinformatycznym w organizacji. Na konkretnych przykładach pokazał, że największym zagrożeniem dla bezpieczeństwa informacji i systemów do ich przetwarzania nie jest skomplikowana technologia lecz czynnik ludzki. Położył nacisk na konieczność uświadomienia pracownikom wartości informacji, jakie pracodawca powierza im do przetwarzania, by mogli realizować swoje zadania.

Duże organizacje o rozbudowanej infrastrukturze teleinformatycznej oprócz informacji o znacznej wartości gospodarczej przetwarzają w swoich systemach dużą ilość danych wrażliwych, szczególnie chronionych prawem. Ich utrata i niewłaściwe wykorzystanie przez osoby trzecie powoduje, że organizacja traci reputację i ponosi wymierne straty finansowe, a osoby odpowiedzialne za jej działalność ponoszą odpowiedzialność karną. Dlatego właśnie takie przedsiębiorstwa powinny powołać w swoich strukturach zespoły CERT (eksperci ds. bezpieczeństwa informatycznego, których głównym zadaniem jest reagowanie na incydenty z zakresu bezpieczeństwa komputerowego) lub korzystać z zewnętrznych usług CERT.

Następnie Karol Szczyrbowski, specjalista w laboratorium informatyki śledczej w firmie Mediarecovery przedstawił metody gromadzenia i zabezpieczania danych w celach dowodowych oraz metody analizy i odzyskiwania danych. Podkreślił, że zabezpieczanie dowodów elektronicznych jest najbardziej krytycznym elementem postępowania ze względu na problem autentyczności i integralności dowodów. W sądzie za autentyczny uznany zostanie tylko taki dowód, co do którego nie ma wątpliwości, że został uzyskany z danego komputera w określonym miejscu i czasie. Dlatego potrzebne są odpowiednie umiejętności i wiedza zarówno na temat zabezpieczania, jak i sporządzania protokołu zabezpieczania dowodów. Jeśli organizacja nie dysponuje odpowiednio przeszkolonymi kadrami, powinna skorzystać z zewnętrznej pomocy, żeby odpowiedzialność poniósł sprawca przestępstwa komputerowego, a nie organizacja czy jej zarząd.

Marta Kusińska z FancyFon pokazała, jak przedsiębiorstwa mogą sprostać wyzwaniom z zakresu bezpieczeństwa mobilnego. Za największe zagrożenia uznała zgubione lub skradzione służbowe lub prywatne urządzenia mobilne, na których znajdują się dane i informacje służbowe oraz nieograniczone możliwości instalowania aplikacji i programów przez użytkowników czy źle lub wcale niezabezpieczone służbowe urządzenia. Tylko jasne reguły i procedury, obowiązujące wszystkich pracowników, z zarządzającymi na czele, mogą zapobiec nieumyślnemu lub świadomemu wyciekowi lub utracie danych. Oddzielenie sfery prywatnej od służbowej stanowi podstawę mobilnego bezpieczeństwa organizacji. Ponadto mobilne urządzenia firmowe powinny łączyć się z serwerami przedsiębiorstwa przez VPN a nie otwartą sieć, a świadomość zagrożeń powinna być powszechna wśród użytkowników.

Media nagłaśniają spektakularne akcje cyberprzestępcze, a społeczne czy sponsorowane akcje informacyjne przestrzegają przed zachowaniami umożliwiającymi bezkarność nielegalnych działań w sieci Internet i o tym mówił w kolejnym wystąpieniu młodszy inspektor Krzysztof Makowski z KW Policji w Poznaniu. Podkreślił, że zadania postawione przed wydziałami i sekcjami do walki z cyberprzestępczością do łatwych nie należą, bowiem mimo pozornej wśród internautów znajomości mechanizmów najpopularniejszych cyberprzestępstw w samym tylko 2014 roku straty spowodowane działalnością przestępczą w Internecie wyniosły na świecie ok. 300 mld dolarów. Tylko powszechna świadomość zagrożeń może podnieść poziom bezpieczeństwa cybernetycznego, dlatego pracodawcy powinni nie tylko wprowadzać mechanizmy i procedury obronne w samych systemach, ale regularnie szkolić pracowników i uodparniać ich na socjotechnikę przestępców.