Halina Świeboda

Zagrożenia bezpieczeństwa współczesnych organizacji

Ekonomiczne Problemy Usług nr 88, 826-834

2012

ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO

NR 703 EKONOMICZNE PROBLEMY USŁUG NR 88 2012

HALINA ŚWIEBODA
Wydział Bezpieczeństwa Narodowego Akademii Obrony Narodowej

ZAGROŻENIA BEZPIECZEŃSTWA WSPÓŁCZESNYCH ORGANIZACJI

Wprowadzenie

Współczesne organizacje działają w niezwykle turbulentnym i mało przewidywalnym otoczeniu, co powoduje, że o wiele bardziej niż w minionych latach narażone są na różnego rodzaju niebezpieczeństwa. Oprócz klasycznych zagrożeń wynikających z istoty i formy prowadzenia działalności, rynku i konkurencji, obok zagrożeń konwencjonalnych pojawiły się zagrożenia wynikające z powszechności stosowania technologii informacyjno-komunikacyjnych. Warunki funkcjonowania organizacji bez względu na ich wielkość i szczebel zorganizowania oraz sektor działania wymagają elastycznego dostosowywania się do potrzeb rynku i w dużej mierze zależą od szybkości i umiejętności wykorzystania informacji.

Medium, które najmocniej wpłynęło na zmianę zachowań, w tym prowadzenia biznesu, jest Internet. Na świecie są ponad dwa miliardy użytkowników Internetu[1]. W krajach Unii Europejskiej ponad 91% korporacji oraz 69% małych i średnich firm posiada strony internetowe, prawie 30% gospodarstw domowych jest podłączonych do Internetu za pomocą szybkich szerokopasmowych łączy.

Według statystki Internet World Status, w Polsce jest 22,5 miliona internautów[2]. Od 2007 roku w trzech kolejnych latach wskaźnik przedsiębiorstw wykorzystujących komputery wzrósł nieznacznie i wynosi 97%, również wskaźnik przedsiębiorstw mających dostęp do Internetu w skali całego kraju wzrastał, osiągając w 2010 roku poziom 96%[3]. Coraz więcej przedsiębiorstw (65,5%) posiada strony

[1] http://unstats.un.org/unsd/wsd/docs/pr/TechNewsDaily.pdf (dostęp online: 18.12.2011).

[2] http://www.internetworldstats.com/stats4.htm (dostęp online: 18.12.2011).

[3] Badanie: *Wskaźniki społeczeństwa informacyjnego*, GUS.

internetowe, a także serwisy internetowe przeznaczone do obsługi handlu elektronicznego. Przynosi to niewątpliwe korzyści dzięki zwiększeniu możliwości dotarcia do konsumentów z całego globu, co przekłada się na zwiększenie udziału w rynku oraz poszerzenie znajomości marki produktów, a to z kolei sprzyja eskalacji przychodów w firmie. Najwcześniej do komunikacji wewnątrz przedsiębiorstwa powszechnie stosowana była infrastruktura sieciowa typu LAN, również intranet, extranet, a w komunikacji z otoczeniem (dostawcy, odbiorcy) wykorzystywana była elektroniczna wymiana danych (poczta elektroniczna) oraz automatyczna wymiana danych w formatach, np. EDI, EDIFACT, ODETTE itp. (78% w 2010 r.).

Spośród 800 tys. abonentów, którzy zarejestrowali nazwy stron internetowych z końcówką .pl, około 63% to przedsiębiorcy. Według Naukowej i Akademickiej Sieci Komputerowej w II kwartale 2011 r. zarejestrowano ponad 70 tys. nowych nazw z domeną .pl. Dynamika wzrostu jest najwyższa w Unii Europejskiej[4].

Rozwijają się intensywnie informatyczne systemy wspomagania zarządzania ERP (11,3% w 2010 r.), CRM (odpowiednio: zbieranie, przechowywanie informacji o klientach oraz zapewnienie dostępu do nich innym komórkom przedsiębiorstwa – 16,4% w 2010 r., oraz analizowanie informacji o klientach w celach marketingowych – 13,1% w 2010 r.).

Przedsiębiorstwa coraz częściej korzystają z możliwości e-administracji, np. w celu pozyskiwania informacji, pobierania formularzy oraz składania ofert w elektronicznym systemie zamówień publicznych (89,3% w 2009 r.).

Rozpowszechnienie technologii informacyjno-komunikacyjnych zrodziło nowe problemy w zakresie bezpieczeństwa zarówno samych systemów, jak i informacji pozyskiwanych, przechowywanych, przetwarzanych i przesyłanych.

1. Ewolucja współczesnej organizacji

Ponad ćwierć wieku temu głównie w praktyce gospodarczej pojawiły się takie zjawiska, jak: (1) powstanie i rozwój transnarodowych korporacji; (2) rozwój automatyzacji procesów produkcyjnych; (3) rozwój systemów komunikacji i technologii informacyjnych. Skutkiem tych procesów, które znacząco wpłynęły na kształt współczesnych organizacji, jak i zarządzania, stała się globalizacja[5], społeczeństwo informacyjne, jako rezultat społecznej dyfuzji innowacji z dziedziny technologii informacyjnych (teleinformatycznych) oraz „nowa gospodarka" (e-biznes) rozwijająca się dzięki rosnącym zasobom wiedzy i wykorzystaniu globalnej infrastruktury teleinformatycznej (Internet). Powiększyło to obszar złożoności, zwiększając dy-

[4] http://www.crn.pl/news/wydarzenia/badania-rynku/2011/09/wiele-polskich-firm-nie-ma-strony-www (dostęp online: 18.12.2011).

[5] Obejmująca przede wszystkim gospodarkę i finanse, politykę i kulturę, a przede wszystkim globalny rynek.

namiczność prowadzenia działań oraz konkurencyjność, jednocześnie powodując wzrost nieprzewidywalności otoczenia i wzrost zagrożeń.

Akceptowanie różnorodności, złożoności i niepewności otoczenia, w którym funkcjonują współczesne organizacje, spowodowało ewolucję oraz pojawienie się nowych struktur organizacyjnych i modeli zarządzania, co wyraża się między innymi nowymi praktykami zarządzania, więziami organizacyjnymi i klimatem organizacyjnym. Ewolucję zarządzania można postrzegać jako ruch „od przewagi formalizacji do przewagi spontaniczności”[6].

Struktury systemów podlegają procesowi zmian organizacyjnych, ewoluując od struktur klasycznych ku strukturom adekwatnym do zmieniających się celów i misji oraz dynamiki i zmian technologicznych w otoczeniu. Współczesne organizacje stają się organizacjami sieciowymi, a wirtualizacja relacji inter- i intrasystemowych to jedna z obecnych strategii rozwoju społecznego, indywidualnego i grupowego[7]. Kształtowanie się organizacji wirtualnych, będących tymczasową siecią niezależnych organizacji (przedsiębiorstw – dostawców, odbiorców, a nawet konsumentów), dzielących koszty, umiejętności i wzajemny dostęp do rynku, wydaje się być trwałą tendencją rozwojową[8]. Podstawowymi cechami charakteryzującymi organizacje sieciowe są: tymczasowość, rozproszenie geograficzne, koncentracja na kliencie, intensywność wykorzystania technologii informatycznych, a także zdolność wykorzystania kluczowych kompetencji uczestników organizacji wirtualnych.

Taka organizacja, korzystając z zalet sieci teleinformatycznej, może stworzyć najbardziej elastyczne możliwości wykorzystania podstawowych umiejętności (*core competences*), dających w danej konfiguracji przewagę konkurencyjną. Jednakże z organizacją wirtualną wiążą się pewne realne niebezpieczeństwa[9]:

- organizacja przystępując do sieci traci kontrolę nad funkcjami przekazywanymi partnerom,
- następuje wzrost zagrożeń informacyjnych (ograniczenie kontroli nad zasobami informacyjnymi),
- istnieje potrzeba budowania zaufania z partnerami z zewnątrz („zarządzanie zaufaniem”).

---

[6] P. Sienkiewicz, H. Świeboda, *Modelowanie organizacji sieciowej w sytuacji zagrożeń dla bezpieczeństwa*, tom I, AON Warszawa 2010, s. 21.

[7] P. Sienkiewicz, H. Świeboda, M. Witecka, *Analiza systemowa organizacji o strukturze sieciowej*, w: *Kooperacje organizacji publicznych*, red. W. Kieżun, A. Letkiewicz, J. Wołejszo, Wyd. WSP, Szczytno 2011, s. 188.

[8] P. Sienkiewicz, H. Świeboda, *Modelowanie…*, *op. cit.*, s. 30.

[9] *Ibidem*.

2. Zagrożenia bezpieczeństwa współczesnych organizacji

Dokonując systemowej analizy zagrożeń dla współczesnych organizacji, wyróżnić można kilka obszarów, w których zagrożenia się pojawiają, a skutki ich realizacji mogą stanowić poważne niebezpieczeństwo dla ciągłości działania podmiotu. Każda organizacja jest narażona na niespodziewane niekorzystne zdarzenia[10]. Przyczyny niektórych zdarzeń niekorzystnych, jak na przykład katastrofy naturalne, najczęściej znajdują się poza kontrolą organizacji. Natomiast w obszarze prowadzonej działalności organizacji związanej z np. finansami istnieje szereg procedur analityczno-ocenowych pozwalających wcześniej rozpoznać symptomy ewentualnych kłopotów, zanim jeszcze kryzys wystąpi.

Poważne następstwa dla ciągłości działania organizacji niosą zagrożenia wynikające z zastosowań technologii informacyjno-komunikacyjnych, wynikające przede wszystkim z zagrożeń dla bezpieczeństwa informacji. Dla bezpieczeństwa systemu zagrożeniem określać będziemy każde zjawisko (proces, zdarzenie) niepożądane z punktu widzenia niezakłóconego działania systemu. Takie zjawiska lub ich kumulacja w określonym miejscu i czasie, oddziałujące destrukcyjnie na system, tworzy sytuacje niebezpieczne dla jego egzystencji (rozwoju). Należy także zwrócić uwagę na możliwość powstawania sytuacji niebezpiecznych dla systemu, będących skutkiem zagrożeń wewnętrznych wynikających np. z zawodności techniki[11]. Zagrożeniem informacyjnym określa się takie zagrożenie, którego skutkiem może być obniżenie (degradacja) wartości zasobów informacyjnych określonej organizacji (obiektu), a w dalszej konsekwencji – obniżenie niezawodności (potencjału) organizacji (obiektu) i obniżenie efektywności działania (skuteczności, ekonomiczności) organizacji.

Wśród cech konstytutywnych, wyróżniających zagrożenia informacyjne, spośród innych należy wyróżnić: brak politycznych i geograficznych granic, anonimowość sprawców, niejasne prawo lub brak uregulowań prawnych, niejasną odpowiedzialność. Trudności w rozróżnieniu aktów dokonywanych w cyberprzestrzeni mogą dotyczyć trudności odróżnienia aktu kryminalnego (cyberprzestępstw) od cyberterroryzmu lub aktu wojny. Do tego typu niebezpiecznej działalności zachęcają sprawców uproszczenia funkcjonalności technologii, czemu towarzyszy spadek cen urządzeń, a także coraz bardziej rozwinięty rynek usług cyberprzestępstw „zdobywania informacji"[12].

---

[10] W 90% incydentów są to tak zwane „ciche katastrofy" – informacja o nich nie zostaje podana do publicznej wiadomości, lecz ich wpływ na działalność organizacji jest znaczny i niszczący, zarówno zasoby, jak i strukturę organizacji.

[11] *Teoria bezpieczeństwa systemów. Synteza doświadczeń*, cz. I, red. P. Sienkiewicz, AON, Warszawa 2004, s. 8.

[12] Karty kredytowe 22%, 0,30–5 USD; konta bankowe 21%, 30–400 USD; hasła do kont e-mail 8%, 1⅓350 USD; programy do wysyłki poczty 8%, 8–10 USD; adresy e-mail 6%, 2–4

Cyberprzestępczość w Polsce powoduje straty do 3 miliardów złotych, a rozwiązywanie problemów i usuwanie szkód zajmowało w Polsce średnio 6 dni rocznie[13]. Najbardziej powszechnym rodzajem cyberprzestępczości w Polsce są wirusy komputerowe i złośliwe oprogramowanie – 64% ankietowanych przyznaje, że doświadczyło tego problemu. Po wirusach kolejne miejsca zajmują oszustwa on-line (20%) i wiadomości wyłudzające dane (phishing, 10%). Od 2011 roku obserwuje się wzrost liczby ataków skierowanych przeciwko różnym organizacjom. Wśród ataków wyróżnia się ataki blokujące na czas nieokreślony dostęp do serwerów korporacyjnych, jak i ataki dokonywane w celu uzyskania nieautoryzowanego dostępu. W obu przypadkach celem jest kradzież danych w celu uzyskania korzyści finansowych, jak również dyskredytacja wizerunku publicznego firmy[14].

Oprócz poznanych zagrożeń naturalnych (np.: pożary, awarie budynków) oraz zagrożeń wynikających z zawodności środków technicznych i programowych szczególne znaczenie mają te, które są rezultatem działalności ludzi. Mniej groźne wydają się zagrożenia niezamierzone, będące konsekwencją niewłaściwego doboru personelu lub wynikające z ich ograniczeń zawodowych (niedostateczne kwalifikacje, brak opanowania określonych procedur itp.). Nie można ich jednak lekceważyć, gdyż ignorancja i arogancja była niemal zawsze przyczyną poważnych katastrof technicznych i technologicznych. Dużo groźniejsze dla firmy są działania zamierzone, których nie można wykluczyć, dokonywane przez pracowników firmy lub kontrahentów, czy „karierowiczów" łamiących prawo. Należy zaznaczyć, że zwykle dysponują oni pewnymi prawami dostępu i posiadają umiejętności w wystarczającym stopniu pozwalające szkodzić[15]. W kolejnych raportach potwierdza się fakt, że właśnie pracownicy stanowią najsłabsze ogniwo w systemach bezpieczeństwa.

USD/MB; serwery Proxy 6%, 0,5–3 USD; pełne dane osobowe 6%, 10–150 USD; informacje o oszustwach 6%, 10 USD na tydzień; numery SSN (social security numbers) 3%, 5–7 USD; Serwery Unix ze złamanymi zabezpieczeniami 2%, 2–10 USD. Źródło: *Raport o zagrożeniach pochodzących z Internet*, tom XII, październik 2007.

[13] Wg badania „Norton Cybercrime Report" firma Symantec podała, że w 2010 r. zidentyfikowała ponad 286 milionów unikalnych odmian złośliwego oprogramowania, co stanowiło wzrost o 19% w porównaniu do 2009 r. (http://norton.com/cybercrimereport, dostęp online: 18.12.2011).

[14] Ewolucja zagrożeń IT w I kwartale 2011 r. Jurij Namiestnikow, http://www.kaspersky.pl/ (dostęp online: 9 czerwca 2011).

[15] Np. z raportu *Computer Crime and Security Survey for 2007* opracowanego przez Computer Security Institute wynika, że właśnie pracownicy stanowią główny powód występowania incydentów związanych z bezpieczeństwem informatycznym. Spośród 500 specjalistów z zakresu bezpieczeństwa 59% stwierdziło, iż w ostatnim roku pracownicy przyczynili się do powstania incydentu zagrażającego bezpieczeństwu informatycznemu w ich organizacji. W badaniu tym uwzględniano m.in. świadome lub nieświadomie udostępnienie danych, wykorzystywanie nielegalnego oprogramowania czy też przeglądanie podejrzanych stron w Internecie. W badaniu zwrócono również uwagę na wzrost liczby kradzieży urządzeń przenośnych, na których znajdowały się dane organizacji.

Zagrożenia zamierzone i świadome są również efektem zorganizowanego działania, którego celem jest destrukcja, tzn. zniszczenie lub zmniejszenie efektywności systemów informacyjnych (lub ich elementów), albo określonych obiektów organizacji tworzących tzw. infrastrukturę krytyczną. Stanowią one nowe wyzwanie dla personelu odpowiedzialnego za bezpieczeństwo organizacji, gotowość systemów informacyjnych, zarządzanie zasobami informacyjnymi itp.[16]

Napastnicy mogą rekrutować się z wywiadu gospodarczego, agencji wywiadu, mogą być to terroryści. Specyficzną grupę stanowią hakerzy, których działania w sytuacji konfliktowej są szczególnie niebezpieczne (tabela 1)[17].

Coraz częściej na styku technologii z rzeczywistością mamy do czynienia z sytuacją, gdy złośliwe oprogramowanie infekuje systemy wpływające bezpośrednio na nasze życie. Niepokojący jest również fakt, że celem wielu ataków stają się firmy zajmujące się bezpieczeństwem IT. Firmy z tej branży obsługują zwykle dużą liczbę klientów, dlatego w wyniku udanego ataku cyberprzestępcy mogą wejść w posiadanie kluczy do cyfrowych portfeli dużej liczby użytkowników rozsianych po całym świecie[18].

Utrata danych może mieć bardzo poważne i nieodwracalne skutki dla organizacji, przynosząc znaczące straty ekonomiczne, konsekwencje prawne i społeczne.

---

[16] P. Sienkiewicz, H. Świeboda, E. Lichocki, *Analiza systemowa zjawiska cyberterroryzm*u, ZN AON nr 2(63), 2006.

[17] Chociaż warto zaznaczyć, że wśród zidentyfikowanych zagrożeń niezwykle ważne są zagrożenia fizyczne, na które narażona jest infrastruktura organizacji czy systemu. Zagrożenia fizyczne mogą realizować się poprzez fizyczne zdobycie dostępu do pomieszczeń oraz poprzez atak w formie kradzieży laptopa, dysków, przeszukiwanie kosza na śmieci w celu znalezienia dokumentacji papierowej. W formie zaawansowanej zagrożenia fizyczne mogą realizować się według scenariuszy, jak np.:

- pokonanie systemu alarmowego, wrażliwego na ruch, z pasywnym detektorem IR (zmiany temperatury), mikrofalami (odbicia);
- złamanie czytnika kart lub zduplikowanie;
- wykorzystanie błędnej weryfikacji przez system biometryczny (wady projektowe), złamanie czytnika odcisków palców, użycie powtórzeń.

Zaawansowane ataki polegają np. na podsłuchiwaniu łączy przewodowych oraz na nagrywaniu wideo i audio, przechwytywaniu obrazu monitora, zdobyciu prywatnych kluczy szyfrujących, mogą to być ataki z wykorzystaniem koni trojańskich.

[18] http://www.viruslist.pl/news.html?newsid=663#2. W przypadku HBGary hakerzy zdołali przeniknąć do sieci firmy poprzez zaatakowanie najmniej krytycznych, a przez to najsłabiej chronionych, serwerów wykorzystywanych przez dział pomocy technicznej. Ponieważ administrator serwera był jednocześnie dyrektorem generalnym firmy, po zdobyciu jego loginu i hasła hakerzy uzyskali również dostęp do różnych innych danych na serwerze. Skradzione dane były bardzo cenne, ponieważ HBGary współpracuje z dużymi organizacjami finansowymi i organami rządowymi. Pierwszy lepszy cyberprzestępca próbowałby od razu sprzedać takie dane na czarnym rynku. Jednak hakerzy stojący za tym atakiem nie poszli utartą ścieżką, zamiast tego publicznie udostępnili uzyskane poufne dane. Ich głównym celem było zaszkodzenie reputacji firmy poprzez rozgłoszenie wiadomości o włamaniu.

Tabela 1

Profile napastników w cyberprzestrzeni

Napastnicy	Motywy	Umiejętności
Wywiad gospodarczy	Konkurencja, finansowe, interesy narodowe	Zaawansowane
Agencje wywiadu	Interesy narodowe	Zaawansowane
Napastnicy wewnętrzni (personel, kontrahenci)	Zemsta, finansowe	Średnio wysokie
Karierowicze	Zdobycie władzy, finansowe	Średnio wysokie
Terroryści	Fanatyzm religijny i polityczny	Zaawansowane
Hakerzy:		
Nowicjusze	Ciekawość chęć wyróżnienia się	Słaba
Black Hat	Ciekawość chęć wyróżnienia się, rzekome zwiększanie bezpieczeństwa	Średnio wysokie
Grey Hat	Do wynajęcia	Zaawansowane
White Hat	Zwiększanie bezpieczeństwa	Średnio wysokie
Hacktivist	Polityczni aktywiści, chcą coś zademonstrować	Zaawansowane

Źródło: na podstawie www.symantec.pl (dostęp online 28.09.2008).

Jednym z głównych zagrożeń dla użytkowników Internetu nadal pozostają infekcje systemu operacyjnego wszelkiego rodzaju szkodliwym oprogramowaniem. Najpopularniejsze są wirusy, konie trojańskie, programy szpiegujące czy też fałszywe oprogramowanie znane także pod nazwą *rogue malware*. Wspólnym mianownikiem dla wymienionych szkodników będzie jednak hasło „zarobek"[19].

Podsumowanie

Bezpieczeństwo współczesnych organizacji w jego głównym nurcie sprowadza się do zarządzania bezpieczeństwem informacji: wytwarzanej, przetwarzanej, przekazywanej i przechowywanej oraz zapewnieniu bezpieczeństwa świadczonych usług. Wzrastająca ilość zagrożeń, wzrost kosztów zabezpieczeń, dylematy między bezpieczeństwem a funkcjonalnością powodują, że coraz trudniej znaleźć właściwe proporcje pomiędzy możliwościami w zakresie przetwarzania, przechowywania i udostępniania informacji a jej ochroną.

Firma Symantec Polska oszacowała koszty przestoju systemów i odzyskania utraconych danych, które wyniosłyby 820 tys. złotych. Symulację przeprowadzono

[19] Raport *Bezpieczeństwo IT w polskich firmach*, Wyd. Webhosting.pl. (dostęp online: 18.12.2011).

dla firmy, która ma 160 komputerów, przy średniej płacy 5 tys. brutto i rocznych przychodach 4 mln[20].

Z niedawno opublikowanych wyników w raporcie *Bezpieczeństwo IT w polskich firmach*[21] wynika, że choć powszechnie stosowane są podstawowe zabezpieczenia w postaci zapór ogniowych i aplikacji antywirusowych, to często przedsiębiorstwa są bezradne wobec skali i różnorodności ataków przeprowadzanych przez cyberprzestępców. Z raportu wynika, że około 40% badanych firm doświadczyło utraty danych.

Warto podkreślić, że niezwykle istotną rolę w bezpieczeństwie odgrywa prowadzenie polityki w organizacjach, której celem jest uświadamianie pracownikom problemów i zagrożeń bezpieczeństwa w tym obszarze. W polskich przedsiębiorstwach tylko w dużych firmach temu problemowi poświęca się nieco więcej uwagi.

Literatura

1. Badanie *Wskaźniki społeczeństwa informacyjnego*, 2009–2010, GUS.
2. http://unstats.un.org/unsd/wsd/docs/pr/TechNewsDaily.pdf (dostęp online: 18.12.2011).
3. http://www.crn.pl/news/wydarzenia/badania-rynku/2011/09/wiele-polskich-firm-nie-ma-strony-www (dostęp online: 18.12.2011).
4. http://www.internetworldstats.com/stats4.htm (dostęp online: 18.12.2011).
5. http://www.viruslist.pl/news.html?newsid=663#2.
6. *Na tym nie warto oszczędzać*, Puls Biznesu (dostęp on line: 7.10.2011).
7. Namiestnikow J., *Ewolucja zagrożeń IT w I kwartale 2011 r.*, http://www.kaspersky.pl/
8. Raport *Bezpieczeństwo IT w polskich firmach*, Wyd. Webhosting.pl (dostęp online: 18.12.2011).
9. Raport *Computer Crime and Security Survey for 2007*.
10. *Raport o zagrożeniach pochodzących z Internetu*, tom XII, październik 2007.
11. Sienkiewicz P., Świeboda H., Lichocki E., *Analiza systemowa zjawiska cyberterroryzmu*, ZN AON nr 2(63), 2006.
12. Sienkiewicz P., Świeboda H., *Modelowanie organizacji sieciowej w sytuacji zagrożeń dla bezpieczeństwa*, tom I, AON Warszawa 2010.
13. Sienkiewicz P., Świeboda H., Witecka M., *Analiza systemowa organizacji o strukturze sieciowej*, w: *Kooperacje organizacji publicznych*, red. W. Kieżun, A. Letkiewicz, J. Wołejszo, Wyd. WSP, Szczytno 2011.

[20] *Na tym nie warto oszczędzać*, Puls Biznesu (dostęp on line: 7.10.2011).

[21] Badanie na temat stanu zabezpieczeń komputerów firmowych w Polsce zrealizowały wspólnie firmy: D-Link oraz home.pl. Raport przygotował i opublikował serwis Webhosting.pl.

14. *Teoria bezpieczeństwa systemów. Synteza doświadczeń*, cz. I, red. P. Sienkiewicz, AON, Warszawa 2004.

SECURITY THREATS OF MODERN ORGANIZATIONS

Summary

Contemporary organizations operate in environment difficult to anticipate. The author of the article considers the issue of present threats to organizations. The threats that emerge from use of ICT were emphasized.

Translated by Magdalena Witecka