Ochrona serwerowni – po pierwsze nie szkodzić

Norbert BARTKOWIAK

Hipokrates sformułował przysięgę składaną do dziś przez adeptów sztuki lekarskiej, której zasadniczym przesłaniem jest „Primum non nocere". „Po pierwsze nie szkodzić" jest ostrzeżeniem dla lekarzy, ponieważ pomóc choremu czasem jest trudno, natomiast zaszkodzić bardzo łatwo. Podstawą jest właściwa diagnoza a potem odpowiednio dobrana terapia. Ważne jest aby zastosowane leki nie tylko wyleczyły, ale także aby nie spowodowały skutków ubocznych. Parafrazując to przesłanie można odnieść je do projektantów projektujących zabezpieczenia przeciwpożarowe, dla tak newralgicznych miejsc, jakimi są serwerownie.

Serwerownia

Trudno sobie wyobrazić współczesną gospodarkę bez usług IT. Wraz z ich rozwojem, rosną potrzeby gromadzenia i przetwarzania danych. Do tego potrzebnych jest wiele serwerów, urządzeń sieciowych i urządzeń do archiwizacji. Duże podmioty i organizacje, aby zapewnić pracę wszystkich wymaganych aplikacji, zazwyczaj koncentrują cały potrzebny sprzęt w jednym miejscu – w Centrum Przetwarzania Danych (EDP – z ang. *Electronic Data Processing*), potocznie zwanymi serwerowniami. Wyposażenie serwerowni może się znacznie różnić, w zależności od potrzeb przedsiębiorstwa czy instytucji z niej korzystającej. Oczywisty wydaje się fakt, że podstawowym elementem, który decyduje o stopniu zaawansowania serwerowni jest wielkość danej instytucji z niej korzystającej oraz charakter prowadzonej przez nią działalności. Zupełnie inne potrzeby będzie mieć niewielka kancelaria doradztwa podatkowego, a inne filia międzynarodowego banku. Im większa i bardziej zinformatyzowana jest firma, tym zazwyczaj większa jest serwerownia. Na największe z nich nierzadko przeznaczany jest oddzielny budynek, podczas gdy najmniejsze zajmują jedno, niewielkie zazwyczaj, pomieszczenie. Serwerownie czy pomieszczenia telekomunikacyjne można podzielić m.in. na stale dozorowane miejscowo oraz wyniesione (np. kontenerowe), bezobsługowe lub raczej obsługiwane zdalnie. Podstawowym elementem każdej serwerowni jest oczywiście umieszczony w niej sprzęt sieciowy i komputerowy. W większości przypadków wszystkie te urządzenia umieszczane są w specjalnych szafach dystrybucyjnych. Ich zadaniem jest zarówno fizyczna ochrona sprzętu sieciowego, jak i porządkowanie elementów infrastrukturalnych. W jednej serwerowni może znajdować się jedna lub wiele szaf, a w każdej z nich – kilka lub kilkanaście serwerów. Serwerownia to nie tylko same urządzenia sieciowe, z serwerami na czele, ale i specjalnie dostosowane pomieszczenie, zapewniające ciągłą pracę systemu teleinformatycznego. Projekt takiego pomieszczenia jest bardzo skomplikowany. Składa się z wielu podsystemów odpowiedzialnych za utrzymanie całości systemu w stanie bezpiecznej pracy.

Rysunek 1. Pomieszczenie z wyposażeniem telekomunikacyjnym (autor: Gregory Maxwell).

Ochrona serwerowni

W pomieszczeniach serwerowni odbywa się transmisja, przetwarzanie i archiwizacja danych. Są to kluczowe procesy dla działalności danego przedsiębiorstwa czy instytucji. Z powodu takiej koncentracji sprzętu, oprogramowania ale przede wszystkim danych w jednym miejscu, najważniejszymi wymaganiami dla serwerowni stają się niezawodność i możliwości transmisyjne. Wystarczy sobie wyobrazić, że scentralizowane usługi przestają działać. Wtedy cała firma, organizacja lub jej klienci nie mają do nich dostępu, nie można korzystać z danych, a to prowadzi do poważnych przestojów procesów biznesowych i poważnych strat. Sektor bankowy czy firmy telekomunikacyjne są przykładem takiego obiektu, który musi utrzymać działalność przez 24 godziny na dobę, siedem dni w tygodniu. Nawet niewielkie przerwy w procesie przetwarzania lub utrata danych, mogą poważnie wpłynąć na ciągłość operacyjną a w wyniku tego na straty ekonomiczne, zwłaszcza w okresach największej liczby transakcji. Średni koszt za godzinę przestoju finansowego domu maklerskiego szacowany jest w USA na 65.000 USD. Jak zatem widać, bezpieczna serwerownia powinna zabezpieczyć dane i procesy, których wartość przekracza wielokrotnie wartość zgromadzonych urządzeń, przed całym spektrum zagrożeń. Zagrożenia można podzielić na zewnętrzne i wewnętrzne. Niebezpieczeństwa, z jakimi możemy mieć do czynienia mogą być spowodowane zarówno przez ludzi (zawirusowanie, nieprawidłowa obsługa, brak doświadczenia, kradzież, wandalizm, sabotaż), jak i wynikać z infrastruktury i technologii (niesprawność lub uszkodzenia okablowania, przerwanie zasilania, uszkodzenie klimatyzacji czy łączności). Wyładowania atmosferyczne powodujące zakłócenia zasilania, pożary czy podtopienia to ostatnia grupa zagrożeń, płynąca ze strony środowiska naturalnego. W zależności od charakteru przetwarzanych i archiwizowanych danych, pomieszczenie serwerowni musi spełniać wiele wymagań organizacyjno-budowlanych, aby zachowany został odpowiedni po-

ziom bezpieczeństwa. Jak już wspomniano, serwerownie bywają różne w zależności od potrzeb. W przepisach zachodnich można znaleźć kategoryzację serwerowni na potrzeby analizy ryzyka dla towarzystw ubezpieczeniowych. Dla przykładu przepisy brytyjskie dzielą serwerownie na pięć kategorii.

Kategoria A: Slight
- nowoczesne małe firmy;
- komputery osobiste – nie pracujące w sieci;
- sprzęt jest standardowy i łatwo wymienialny;
- operacje mogą być przenoszone w inne miejsce bez większych trudności;
- najważniejsze pliki mogą być archiwizowane okresowo, na przykład na dyskietce / dyski zip lub CDR;
- możliwość wystąpienia przerwy w działalności gospodarczej jest niewielka.

Przykład: typowe małe biura, pracownie projektowe.

Kategoria B: Low
- nowoczesne komercyjne / przemysłowe środowiska;
- komputery osobiste – pracujące w sieci;
- sprzęt jest standardowy i łatwo wymienialny;
- operacje mogą być przenoszone do innej lokalizacji z trudem;
- pliki mogą być archiwizowane okresowo na centralnym serwerze;
- utrata danych może wystąpić na wielu komputerach lub centralnym serwerze;
- możliwość przerwania działalności jest niska.

Przykład: typowe małe i średnie przedsiębiorstwa mające działy handlowe, centralne systemy wspomagania projektowania CAD / CAM, stanowiska Call Centre, w których ważne pliki mogą być okresowo archiwizowane na centralnym serwerze.

Kategoria C: Moderate
- wydzielone pomieszczenie dla urządzeń;
- centralny serwer/y;
- sprzęt jest standardowy, ale wymiana wymaga zwłoki czasowej;
- operacje mogą być przenoszone do innej lokalizacji z trudem;
- pliki mogą być archiwizowane na centralnym serwerze okresowo;
- przerwa wpływa na krótkoterminowe operacje biznesowe.

Przykład: urządzenia telekomunikacyjnych Call Centre mające alternatywne lokalizacje.

Kategoria D: High
- wydzielone pomieszczenie/a dla urządzeń;
- centralny serwer/y;
- urządzenia mogą być nietypowe i wymiana wymaga zwłoki czasowej;
- trudny transfer procesów do innych lokalizacji bez precyzyjnych planów awaryjnych;
- pliki mogą być archiwizowane na centralnym serwerze okresowo;
- przerwa wpływa średnioterminowo na działalność gospodarczą.

Przykład: główne obiekty telekomunikacyjne, w przemyśle – komputerowe centra sterowania produkcją.

Kategoria E: Critical
- wydzielone obiekty dla urządzeń;
- centralny serwer/y, sprzęt telekomunikacyjny;
- sprzęt jest wysokiej wartości lub specjalnej konstrukcji – niewymienny;
- transfer procesów nie jest możliwy bez precyzyjnych i regularnie testowanych planów awaryjnych;
- kopie zapasowe danych są tworzone w sposób ciągły na centralnym serwerze;
- przerwa w pracy jest niedopuszczalna.

Przykład: centra przetwarzające operacje finansowe, centra kontroli ruchu lotniczego; systemy nadzoru i sterowania w przemyśle chemicznym czy elektrowniach jądrowych.

W zależności od zagrożeń, przed którymi należy chronić serwerownie, projekty budowlane pomieszczeń serwerowni uwzględniają np. odpowiednią odporność wydzieleń budowlanych na przebicie, ekranowanie elektromagnetyczne czy odporność na działanie wysokich temperatur. Pomieszczenia często muszą być chronione przed dostępem osób nieuprawnionych. W przypadku centrów przetwarzających operacje finansowe, serwerownia traktowana jest podobnie jak skarbiec, bowiem dane w tym przypadku traktowane są jak wartości pieniężne. Osobnym problemem jest ochrona systemu informatycznego od zagrożeń wewnętrznych, do których w dużej mierze zalicza się błędy ludzkie oraz awarie które mogą spowodować przerwę w pracy systemu. Projekt serwerowni, w zależności od charakteru danych jakie przetwarza i przechowuje, musi uwzględniać obowiązujące przepisy, a jest ich sporo. Poza przepisami dotyczącymi ochrony przeciwpożarowej, serwerownie muszą spełniać wymagania aktów prawnych określających wymagania na ochronę bezpieczeństwa teleinformatycznego i przetwarzanych informacji. Są to m.in.:

Dz. U. nr 11, poz. 95 z 08. 02. 1999 r. – Ustawa o ochronie informacji niejawnych – określa zasady ochrony informacji, które stanowią tajemnicę państwową lub służbową. Przepisy ustawy mają zastosowanie do organów władzy publicznej, sił zbrojnych Rzeczypospolitej Polskiej i ich jednostek organizacyjnych, Narodowego Banku Polskiego i banków państwowych, państwowych osób prawnych, przedsiębiorców, jednostek naukowych lub badawczo-rozwojowych, których działalność związana jest z dostępem do informacji niejawnych.

Dz. U. 2005 nr 171 poz. 1433 – Rozporządzenie Prezesa Rady Ministrów z 25 sierpnia 2005 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego – organizacja ochrony bezpieczeństwa teleinformatycznego m.in. obejmuje ochronę fizyczną, elektromagnetyczną i kryptograficzną; zapewnienie niezawodności transmisji oraz kontrolę dostępu do urządzeń systemu lub sieci teleinformatycznej.

Dz. U. nr. 133, poz. 883, z późn. zm. – Ustawa o ochronie danych osobowych z 29 sierpnia 1997 r.

Dz. U. 2004 nr 100 poz. 1024 – Rozporządzenie ministra spraw wewnętrznych i administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Dz. U. 1997 nr 114 poz. 740 Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia.

Dz. U. 1998 nr 129 poz. 858 – Rozporządzenie ministra spraw wewnętrznych i administracji z 14 października 1998 r. w sprawie szczegółowych zasad i wymagań, jakimi powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne.

Dz. U. 2002 nr 144 poz. 1204 – Ustawa z 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną.

Dz. U. 2004 nr 236 poz. 2364 – Rozporządzenie Rady Ministrów z 26 października 2004 r. w sprawie sposobu tworzenia, utrwalania, przekazywania, przechowywania i zabezpieczania dokumentów związanych z czynnościami bankowymi, sporządzanych na elektronicznych nośnikach informacji.

Dz. U. 2003 nr 116 poz. 1090-Rozporządzenie Rady Ministrów z 24 czerwca 2003 r. w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony.

Ochrona przeciwpożarowa

W dalszej części artykułu skoncentrowano się na ochronie przeciwpożarowej skupiającej się przede wszystkim na wczesnym wykrywaniu i lokalizowaniu zagrożeń. Rozwiązania w zależności od wielkości i charakteru serwerowni będą się różnić. Generalnie ochrona polegać powinna na jak najwcześniejszym wykryciu potencjalnego zagrożenia i w zależności od wykrytego stadium, podjęcia odpowiednich kroków mających na celu zlikwidowanie przyczyny i ewentualnych skutków. Wykrywanie dymu w centrum przetwarzania danych jest najważniejszym elementem ochrony przeciwpożarowej i stanowi poważne wyzwanie dla ☞

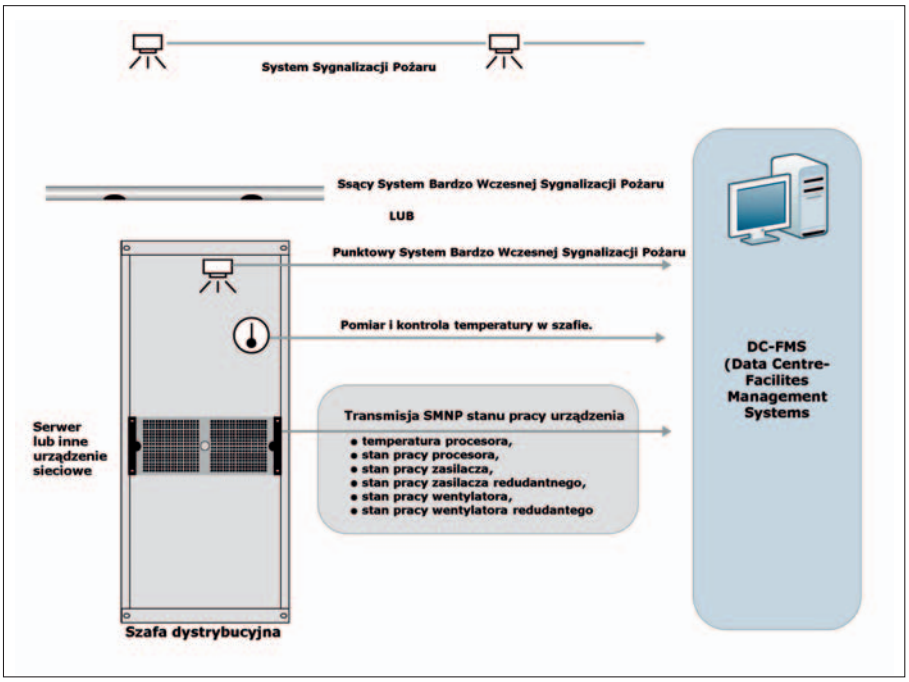
projektanta z powodu niewielkiej ilości dymu oraz dynamiki przepływu powietrza. Należy mieć jednak na uwadze, że nawet niewielka ilość dymu i oparów z przegrzanych elementów i przewodów może prowadzić do uszkodzenia wrażliwych urządzeń elektronicznych. Produktami ubocznymi dymu z tlących się izolacji przewodów, jak i płytek elektronicznych są gazy, które w atmosferze tworzą opary takich związków jak HCL (kwas solny) doprowadzających do korozji wrażliwych elementów elektronicznych. Już wytworzenie niewielkiej ich ilości, jak 16 mg, może skutkować w dłuższym okresie korozją i uszkodzeniem urządzeń elektronicznych. Statystyki amerykańskie wykazują, że przegrzania elementów tylko w ok. 5% stanowią bezpośrednią przyczynę awarii, polegającą na uszkodzeniu przegrzanego elementu. W pozostałych przypadkach przyczyną były dym i gazy powstałe podczas przegrzewania się urządzeń czy kabli, w tym HCL. Istotny jest również fakt, iż etap tlenia elektroniki może trwać wiele godzin lub nawet dni. Energia wydzielana podczas tlenia płyty elektroniki jest mniejsza lub równa 1,0 kW. Dla porównania, energia cieplna uwalniana podczas pożaru biurowego kosza na śmieci może być w przedziale od 15 KW nawet do 100 KW. Źródłem powstania dymu, a nawet ognia, mogą być oprócz urządzeń, przeciążone kable, a szczególnie miejsca ich połączeń, w tym wszelkie złącza, które wskutek złego montażu utleniają się i stają się elementem oporowym. Takie złącze zaczyna się grzać wskutek wzrostu rezystancji i wytracania na nim energii elektrycznej. Wykrywanie dymu w warunkach serwerowni nie jest rzeczą prostą, ale wykonalną. Przede wszystkim należy w miarę możliwości nie dopuszczać do sytuacji, w których może nastąpić wydzielanie się dymu. Zacząć więc należy od nieustannego monitorowania pracy urządzeń i wykrywania wszelkich odstępstw od stanu normalnego.

Monitorowanie parametrów – Data Centre – Facilities Management Systems

Wg tzw. prawa Moore'a, moc obliczeniowa komputerów podwaja się co trzy lata. Wynika to z rozwoju technologii pozwalających na coraz większe upakowanie tranzystorów na tej samej powierzchni krzemu. Zwiększa się tym samym gęstość mocy wydzielanej na procesorze. O ile pierwsze procesory komputerów klasy PC AT wydzielały moc rzędu dziesiątek watów, o tyle współczesne, wielordzeniowe procesory wydzielają setki watów na tej samej powierzchni. Tak wysokie obciążenie cieplne wymaga wymuszonego chłodzenia już samego procesora. Z tego powodu w obudowie serwera montuje się wentylator, a nawet kilka redundantnych wentylatorów. Ciepło wyprowadzane jest z poszczególnych obudów urządzeń zamontowanych w szafie dystrybucyjnej, a następnie z całego pomieszczenia poprzez system wentylacji i klimatyzacji pomieszczenia CRAC (ang. *Computer Room Air Conditioning*). Awaria wentylatora chłodzącego procesor może oznaczać, że za chwilę nastąpi przegrzanie procesora lub innego elementu, na którym wydziela się ciepło. Skutkować to może awarią serwera, a w najgorszym razie spaleniem płyty i wydzieleniem gazów, które mogą zanieczyścić pozostałe urządzenia, zamontowane w tej, jak i w sąsiednich szafach dystrybucyjnych. Współczesne komputery i inne urządzenia peryferyjne, pracujące w sieci, komunikują się ze światem zewnętrznym zestandaryzowanym protokołem komunikacji SNMP (ang. *Simple Network Management Protocol*). Komunikując się z całą siecią urządzeń można otrzymywać dane o stanie pracy każdego z nich, w tym także informacje o awariach. Można np. na bieżąco odczytywać temperaturę procesora, status pracy wentylatora/ów chłodzących procesor. Monitorowaniem stanu poszczególnych parametrów zajmują się systemy DC-FMS (*Data Centre-Facilites Management Systems*) wspomagające pracę personelu nadzorującego lokalnie czy zdalnie pracę urządzeń w serwerowni. Systemy DC-FMS automatycznie alarmują o awariach i wszystkich sytuacjach, które mogą skutkować przerwą pracy poszczególnego urządzenia a w szczególnym przypadku, początkiem przegrzewania się danego elementu. Do systemów DC-FMS podłącza się również czujniki mierzące temperaturę w szafie dystrybucyjnej, a także systemy sygnalizacji pożaru. W przypadku pojawienia się sygnału alarmowego obsługa wspierana jest wizualizacją wskazującą miejsce pojawienia się np. wyższej temperatury, awarii czy dymu.

Systemy bardzo wczesnej sygnalizacji pożaru

Takie urządzenia, jak serwery, switche, rutery itp. montowane są w tzw. szafach dystrybucyjnych. Zwykle każda szafa ma wymuszony obieg powietrza, niezależnie od lokalnych wentylatorków schładzających procesory w obudowie serwera. Odpowiednie warunki do pracy urządzeń telekomunikacyjnych i serwerów zapewniają systemy CRAC (ang. *Computer Room Air Conditioning*), które odpowiadają za odpro-



Rysunek 2. Przykład możliwych źródeł informacji pozwalających na stałe monitorowanie pracy serwerowni.

wadzanie ciepła z pomieszczenia serwerowni. W tego typu pomieszczeniach zapewnia się od 10 do nawet 100 wymian powietrza na godzinę, a prędkość przepływu powietrza dochodzi do 1m/s. Łatwo sobie wyobrazić, jak wielkiemu rozrzedzeniu ulegnie niewielka ilość dymu powstałego wskutek tlącego się np. rezystora na płycie elektroniki, czy przeciążonego przewodu zasilającego. Kiedy mimo kontroli parametrów pracy dojdzie do sytuacji, w której nastąpi wydzialanie dymu powinien on zostać wykryty przez czujki dymu. Oczywiście, przy tak niewielkich ilościach dymu musi być zastosowana odpowiednio czuła technologia. Czułość czujki dymu jest definiowana w kategoriach zaciemnienia (ang. *obscuration*) w procentach na metr (% obs./m.) – oznacza to ilość dymu, która przesłoni światło w procentach na odcinku o długości jednego metra. British Fire Protection Systems Association definiuje trzy kategorie czułości do systemów wykrywania dymu:

- normalny: czułość wyższa niż 5% obs./m,
- średni: czułość wyższa niż 2% obs./m,

• wysoki: czułość wyższa niż 0,8% obs./m.

Dostępne na rynku systemy wykrywanie pożaru mają bardzo szeroki zakres czułości (patrz tabela 1). Trzy czynniki powinny być uwzględnione przy określaniu wymaganej czułości systemu wykrywania:

a) wrażliwość urządzeń na uszkodzenia w wyniku przegrzania,
b) szybkość reakcji personelu, gdy wystąpi alarm,
c) rodzaj i skuteczność środków do walki z pożarem (podręczny sprzęt lub automatyczny SUG).

Punktowe czujki bardzo wczesnej detekcji dymu

Punktowe czujki bardzo wczesnej detekcji dymu wyglądem przypominają czujki optyczne klasycznych systemów. Jednak ich wewnętrzna konstrukcja jest znacznie bardziej skomplikowana. W komorze czujki laserowa dioda emituje impulsy światła 10 000 razy silniejszego od światła typowej diody LED. Strumień światła przechodzi przez komorę pokrytą lustrzaną powłoką. Kształt komory przypomina przecięty walec, na końcu którego znajduje się czujnik fotoelektryczny. Jeżeli nic nie znajdzie się na drodze strumienia światła, wpada on w pułapkę światła specjalnej konstrukcji (rys. 4). Jeśli cząstka dymu (lub kurzu) dotrze do komory, wtedy światło lasera jest rozproszone i odbijając się wielokrotnie od ścianek komory pada na czujnik fotoelektryczny. System w oparciu o opatentowane algorytmy analizy światła rozproszonego ustala, czy przyczyną rozproszenia światła jest kurz, czy dym. W przypadku kiedy źródłem jest dym, następuje przeliczenie stężenia i porównanie z dokonaną nastawą progów alarmowych. Przekroczenie zadanych progów sygnalizowane jest alarmem. Do dyspozycji zwykle jest kilka (2-3) progów alarmowych.

Tabela 1. Podział czujek pożarowych ze względu na czułość wyrażoną w przezroczystości [%] /m

Typ czujki	Przedział czułości
Jonizacyjna	2.6–5.0 %/m
Fotoelektryczna	6.5–13.0 %/m
Liniowa	3 %/m
System ssący	0.005–20.5 %/m
Punktowa czujka laserowa	0.06–6.41 %/m

Testowanie systemu bardzo wczesnej detekcji dymu

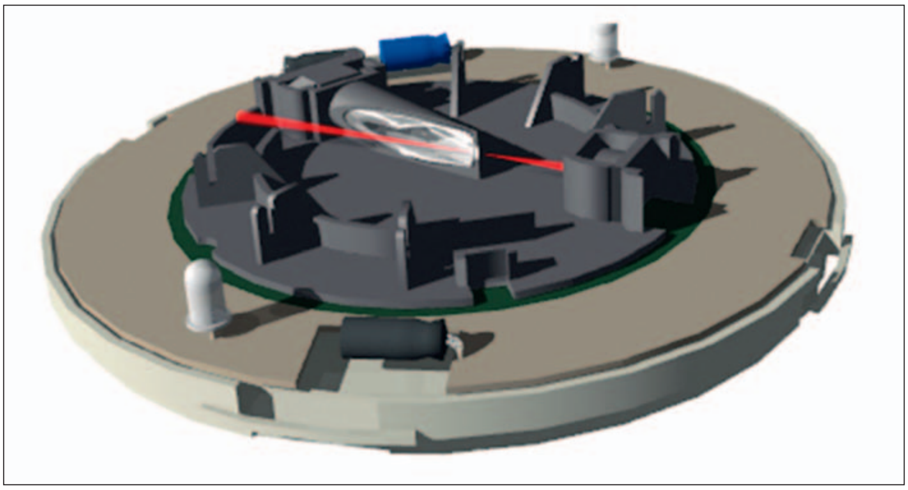
Aby mieć pewność co do prawidłowo zastosowanych rozwiązań należy dokonać walidacji, czyli sprawdzenia działania. Obecnie ocenę systemu bardzo wczesnej detekcji dymu doko-

Czujki w powszechnie stosowanych systemach sygnalizacji pożaru wg norm brytyjskich i amerykańskich zaliczane są do klasy EWSD (ang. Early Warning Sensor) natomiast w systemach ekstremalnej czułości, jako VEWSD (ang. Very Early Warning Sensor). Systemy VESD dedykowane są do ochrony cennych urządzeń elektronicznych i elektrycznych. Systemy VESD generalnie dzielą się na dwa rodzaje rozwiązań technicznych: systemy ssące lub podobnie jak w przypadku klasycznych systemów, czujki punkowe. W obu przypadkach stosuje się bardzo zaawansowane technologie, bowiem przy tak ekstremalnych czułościach istnieje znacznie większe ryzyko wywołania fałszywego alarmu. W tym celu stosuje się bardzo skomplikowane algorytmy obliczeniowe w celu odfiltrowania wszelkich zjawisk zakłócających wykrycie dymu w tak mikroskopijnych ilościach.

Systemy zasysające bardzo wczesnej sygnalizacji pożaru

Systemy wykrywania dymu zasysające różnią się od systemów opartych o czujki punktowe. Podstawową częścią systemu zasysającego jest specjalna komora analizująca, o bardzo wysokiej czułości (0.005 %/m). Do tej komory specjalna pompa zasysa powietrze poprzez system rur wyposażonych w otwory, tzw. kapilary. System rur rozprowadzony w strefie dozorowanej tworzy matrycę otworów, traktowanych jak czujka punktowa. Rzeczywista czułość dla otworu ssącego jest niższa, zależy od liczby otworów i udziału procentowego przepływającego przezeń powietrza w stosunku do całego zasysanego powietrza. Nie mniej jest to nadal bardzo wysoka czułość (patrz tabela 1).

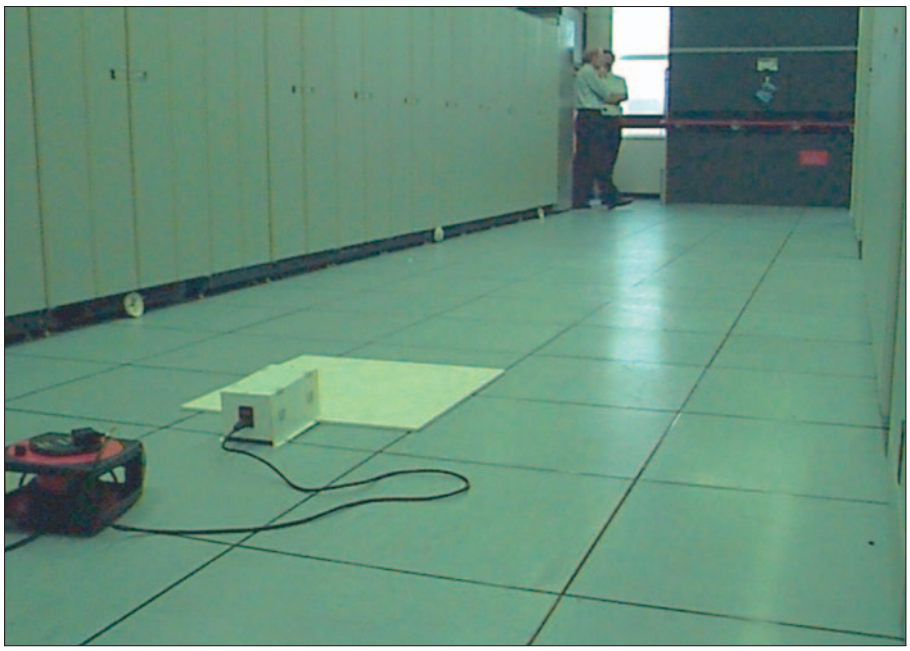
Rysunek 3. System ssący zainstalowany na szafach z urządzeniami telekomunikacyjnymi w centrali telefonicznej.



Rysunek 4 Punktowa, laserowa czujka systemu bardzo wczesnej sygnalizacji pożaru.

☞

nuje się praktycznie w miejscu zainstalowania. Do testowania systemów bardzo wczesnej detekcji stosuje się test potocznie zwany „Testem gorącego przewodu" (ang. Hot wire test). Polega on na przepuszczeniu prądu w krótkim odcinku przewodu pokrytego PCV, który produkuje niewielką ilość ledwo widocznego szarego dymu i symulację pożaru tlącego się znacznie mniej niż 1,0 kW. Jako źródło prądu stosuje się zasilacz sieciowy z wyjściem 6V napięcia przemiennego (AC) i wydajności prądowej 15A. Normy brytyjskie zalecają przeciążenie przez 60 s przewodu o długości 1 m i przez 180 s przewodu o długości 2 m. W standardzie amerykańskim również zaleca się test z przegrzewaniem przez 60 s dwóch odcinków przewodu 2 x 1 m, połączonych równolegle. Przewód jest wiązką drutów 10/0,1 mm (przekrój przewodu 0,078mm^2) w izolacji z PVC o grubości promieniowej 0,3 mm. Zazwyczaj badanie przeprowadza się w pomieszczeniu, w trakcie procesu uruchamiania systemu. Reakcja systemu (sygnalizacja przekroczenia nastawionego progu alarmowego) powinna nastąpić nie później niż 60 – 120 s od momentu odłączenia zasilania przewodu.



Rysunek 5. Test „gorącego przewodu" przeprowadzany w centrali telefonicznej.

Środki tłumienia pożaru

Jeśli zostaną podjęte działania na etapie bardzo wczesnej detekcji dymu, można zapobiec dalszemu przegrzaniu danego elementu czy urządzenia (np. przez wyłączenie zasilania). Wtedy uszkodzenia sprzętu elektronicznego są minimalne a czas reakcji bardzo szybki. Systemy standardowej czułości (powszechnie stosowane), mogą być stosowane tylko do wykrywania pożaru, gdy ogień i dym może już spowodować pewne uszkodzenia wrażliwych urządzeń. Na tym etapie pożar, jeżeli nie zostanie powstrzymany w stosunkowo krótkim czasie, może rozwijać się szybko i rozprzestrzeniać na całe pomieszczenie. Zakładając, że serwerownia nadzorowana i monitorowana jest nieustannie przez przeszkolony personel, niezbędnym (w wielu przypadkach wystarczającym) wymogiem wydaje się wyposażenie pomieszczeń w gaśnice przenośne na dwutlenek węgla (CO_2) lub inny „czysty" gaz. Gaśnice powinny być zlokalizowane w pobliżu urządzeń elektronicznych dla ułatwienia szybkiego stłumienia ewentualnego pożaru w fazie początkowej. Odległość z dowolnego miejsca do najbliższej gaśnicy nie powinna przekraczać 15 m. W obiektach bez stałego dozoru, gdzie czas ewentualnej reakcji polegającej na inspekcji miejsca zagrożenia będzie zbyt długi, stałe urządzenia gaszące, działające na zasadzie wyparcia tlenu z atmosfery, wydają się wtedy nieodzowne. Proces gaszenia a raczej tłumienia pożaru uruchamiany jest z pewnym opóźnieniem, po wykryciu pożaru przez co najmniej dwie czujki pracujące na różnych liniach dozorowych (koincydencja – przyp. autora). W tym czasie zamykane są otwarte w strefie gaszenia okna i drzwi, zamykane przeciwpożarowe klapy odcinające, wyłączane są systemy CRAC oraz ewakuowani są ludzie z pomieszczeń objętych pożarem. Odcinane jest również zasilanie urządzeń serwerowni, co nie jest rzeczą prostą gdy wszystkie urządzenia zasilane są ze źródeł rezerwowych, jak UPS a nawet generatory. Rozważania na temat rozwiązań polegających na tłumieniu ognia wymagają oddzielnego omówienia. Istotną sprawą jest moment uruchomienia tego typu środków. Jest to ostatni z możliwych poziomów alarmowania, będących do dyspozycji pośród wszystkich rozwiązań.

Wielostopniowa skala alarmowania

Przypadek każdej serwerowni należy rozpatrywać indywidualnie. Przyjmując na potrzeby tego artykułu sytuację, w której zastosowano wszystkie omawiane rozwiązania, można zbudować kilkustopniową skalę ostrzegania i alarmowania (patrz tabela 2). Jak wspomniano wcześniej, powstawanie zagrożenia może mieć charakter długotrwały, odstępy w czasie między pojawieniem się np. ostrzeżenia o wysokiej temperaturze a sygnalizowaniem pojawienia się pierwszych cząstek dymu może wynosić tygodnie. Ważne jest, aby nie lekceważyć żadnego z sygnałów i reagować na nie zgodnie z opracowanymi procedurami. Ważne też jest

Alarm koincydenty z SSP	•Druga (koincydentna) czujka systemu SSP potwierdziła obecność dymu. Poziom wyzwalania SUG.
Alarm z czujki SSP	•Potwierdzenie przez SSP pojawienia się dymu w obszarze dozorowania czujki.
Alarm wstępny z SSP	•Pojawienie się prawdopodobne dymu w obszarze dozorowania czujki.
Alarm z VEWSD	•Pewne pojawienie się niewielkiej, ciągle niewidocznej ilości dymu.
Alarm wstępny z VEWSD	•Pojawienie się prawdopodobnie niewielkiej ilości dymu w obszarze dozorowanym.
Alarm z DC-FMS	• Przekroczenie bezpiecznego progu temperatury wewnątrz szafy dystrybucyjnej.
Alarm z DC-FMS	•Sygnał o przekroczeniu parametrów pracy danego urządzenia.

Tabela 2. Dostępnych progów ostrzegania i alarmowania o zagrożeniu pożarowym.

wykrywanie trendu danego zjawiska. Powolne ale ciągłe narastanie temperatury wskazuje jednoznacznie na to, że sytuacja zmierza w niebezpiecznym kierunku.

Podsumowanie

Strategia ochrony serwerowni polega przede wszystkim na ochronie mienia, jakim są dane i procesy ich przetwarzania na sprzęcie komputerowym, a w drugiej kolejności samego wyposażenia serwerowni. Należy chronić przed powstaniem najmniejszego nawet źródła dymu. Powstanie zalążku otwartego ognia w serwerowni odpowiedzialnej za procesy gwarantujące bezpieczeństwo ludzi (np. centra kontroli lotów), czy mienia znacznej wartości (np. centra finansowe) jest niedopuszczalne, a pożar, który w konsekwencji spowoduje wyłączenie z eksploatacji serwerownie jest nie do zaakceptowania. Uwzględniając wielkość i kategoryzując ryzyko dla danej serwerowni należy podczas projektowania zabezpieczenia sięgać w pierwszej kolejności po rozwiązania techniczno-organizacyjne pozwalające na szybką i kompetentną reakcję na wczesne symptomy potencjalnego zagrożenia. W planach ochrony należy uwzględnić udział personelu obsługi serwerowni, który jako jedyny ma dostęp do jej pomieszczeń i często przebywa w nich lub w pobliżu przez 24 godz/dobę. Profesjonalnie przygotowany personel, jeśli zostanie odpowiednio ostrzeżony o powstającym zagrożeniu i wsparty informacją z systemu zarządzającego DC-FMS o charakterze zagrożenia i miejscu jego wystąpienia, może natychmiast podjąć odpowiednie działania. Przy powszechnie stosowanej technologii wirtualizacji serwerów, budowania redundantnych systemów schładzania procesora, nie jest problemem szybka podmiana „podejrzanego" elementu. Stosowanie radykalnych środków powinno być brane pod uwagę ze świadomością, że jest to ostateczność, generującą określone skutki.

Źródła:
1. How Early Warning Fire detections Works – Rakesh Dogra, The Data Center Jurnal, 18 September 2008.
2. (Source: Steven R. Christensen and Lawrence L. Schkade, „Financial and Functional Impact of Computer Outages on Business", University of Texas at Arlington).
3. Spot and Aspirated Laser Smoke Detection in Telecommunications Facilities Daniel T. Gottuk and Lawrence A. McKenna.
4. Innovative VID Smoke Detection Technology, Daniel J. O'Connor, P. E., Chief Technical Officer, Schirmer Engineering, Fire Protection Engeennering, 1/2010.
5. Rozwiązania technologiczne systemu View przenoszą nas w XXI wiek – Cezary Krupa, Systemy Alarmowe 3/97.
6. Zagadnienia przeciwpożarowe w stacjach transformatorowych SN -Janusz Sawicki, elektro. info 11/200.
7. BS 6266: 2002 Code of practice for fire protection for electronic equipment installations.
8. NFPA 75: Standard for the Protection of Information Technology Equipment, 2009 Edition.
9. NFPA 76: Standard for the Fire Protection of Telecommunications Facilities, 2005 edition.
10. VESDA – VTT 100 User Manual.
11. Laser Technology Smoke Detector – System Sensor, Applications Guide.
12. W artykule wykorzystano fotografię: Telecommunications equipment in one corner of a small data center. Contributed and licensed under the GFDL by the photographer, Gregory Maxwell.