



Pomieszczenia kluczowe pod ochroną



W nowoczesnej gospodarce
najważniejsza jest informacja.
Coraz częściej o istnieniu
przedsiębiorstwa decyduje
stopień wykorzystania
nowoczesnych technologii.

Krzysztof Kowalczyk
Hestia Loss Control,
specjalista ds. oceny ryzyka,
zajmuje się zagadnieniami ryzyka
ogniowego i utraty zysku,
inżynier, absolwent Szkoły Głównej
Służby Pożarniczej w Warszawie,
w Grupie Ergo Hestia od 1994 roku.

Dzisiaj trudno jest sobie wyobrazić pracę bez komputera lub urządzeń posiadających układy scalone. Z dużą odpowiedzialnością można stwierdzić, że układy scalone - ich podstawowe elementy - zdominowały nasze życie prywatne i zawodowe. Obecnie towarzyszą nam w zasadzie wszędzie, począwszy od bardzo popularnych pendrive'ów, wszechobecnych telefonów komórkowych, aparatów cyfrowych, czy pecetów, a skończywszy na zaawansowanych technologicznie serwerach wykonujących skomplikowane operacje logiczne. Coraz częściej o istnieniu przedsiębiorstwa decyduje stopień wykorzystania nowoczesnych technologii. Informacje, a co za tym idzie i wiedza, przetwarzane są w taki sposób, aby stworzyć jak najlepszy i najbardziej konkurencyjny produkt.

Nie uświadamiamy sobie tego na co dzień. Gdy na przykład chcemy wysłać e-maila czy skorzystać z wyszukiwarki internetowej, zawsze używamy co najmniej jednego serwera. Podobnie w przypadku skomplikowanych systemów sterujących dużą liczbą procesów technologicznych z zastosowaniem automatyki przemysłowej. Mało kto zastanawia się nad tym, gdzie znajduje się „serce” systemu oraz jak przebiega transmisja informacji. Najważniejszy jest postawiony cel, czyli to, co zamierza się osiągnąć.

Co to są pomieszczenia kluczowe?

W każdym nowoczesnym przedsiębiorstwie istnieje jedno lub kilka miejsc odpowiedzialnych za wszelkie czynności związane z procesami cyfrowego „obrabiania” informacji. Są to wszelkiego rodzaju serwerownie, sterownie, nastawnie, centrale telefoniczne itp. Połączenie z nimi istnieje za pomocą sieci transmisyjnej, którą tłoczy się informacje do systemu.

Na całym globie znajdują się miliony takich kluczowych pomieszczeń: przede wszystkim serwerowni i central telefonicznych - zlokalizowanych w lepiej lub gorzej zabezpieczonych pomieszczeniach. Codziennie są one narażone



W kraju spotyka się firmy, których wszelkiego rodzaju serwerownie, sterownie, nastawnie oraz centrale telefoniczne zabezpieczone są zgodnie z najlepszymi światowymi standardami, gdzie poziom świadomości menedżerów IT jest bardzo wysoki.

na różne rodzaje ryzyka (np. pożar, kradzież, zalanie, przepięcie itp.), powodujące znaczne szkody.

Brak odpowiednich zabezpieczeń lub ich nieodpowiednie stosowanie w najlepszym przypadku uniemożliwi nam wysłanie e-maila, w gorszym wstrzyma procesy produkcyjne, skutkujące na przykład brakiem energii elektrycznej w gniazdkach naszego mieszkania. W wydawałoby się najgorszym dla nas razie - uniemożliwi przeprowadzanie transakcji finansowych i to akurat w momencie dokonywania przelewu w celu opłacenia naszej wymarzonej podróży w systemie Last Minute w Bory Tucholskie lub romantycznej kolacji w restauracji przy plaży w Sopocie. Niezbyt przyjemna perspektywa!

Dlatego warto przez chwilę zastanowić się, jak winny być zabezpieczane pomieszczenia ze sprzętem elektronicznym o znacznej wartości, odpowiedzialnym za wykonywanie czynności i procesów o żywotnym znaczeniu dla przedsiębiorstw.

Artykuł niniejszy koncentruje się na problemach związanych z ochroną sprzętu w sensie fizycznym, pozostawiając ochronę sieci i oprogramowania, która jest odrębną kwestią.

Świadomość menedżerów IT

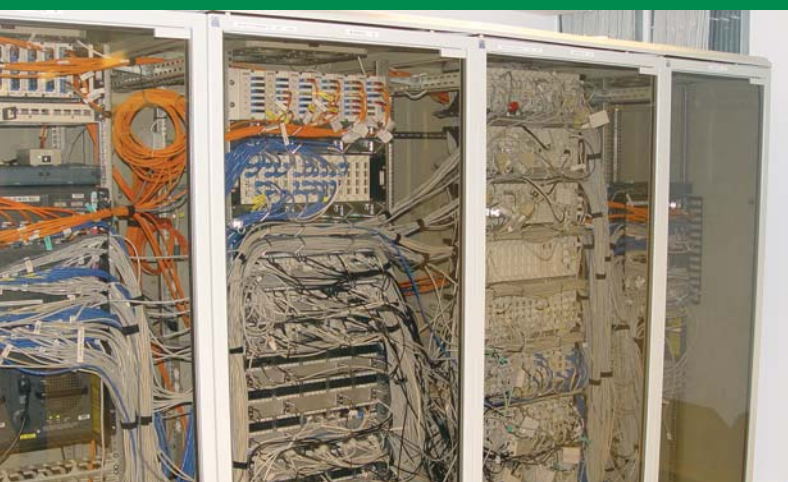
Dotychczasowe doświadczenia związane z oceną ryzyka pozwalają na twierdzenie, że poziom stosowanych zabezpieczeń jest różny, ale przeważnie powiązany ze świadomością zagrożeń wśród osób odpowiedzialnych za procesy IT. Nie należy także zapominać o aspektach finansowych, odgrywających decydującą rolę przy podejmowaniu decyzji o inwestycjach w środki

bezpieczeństwa. Niemniej i tu występują liczne przypadki działań, zaskakujących i jednocześnie trudnych do racjonalnego wytlumaczenia.

W kraju są firmy, których serwerownie, sterownie, nastawnie oraz centrale telefoniczne zabezpieczone są zgodnie z najlepszymi światowymi standardami, a poziom świadomości menedżerów IT jest bardzo wysoki. Zdarza się jednak, że pomieszczenia ze sprzętem komputerowym odpowiedzialnym za funkcjonowanie całych organizmów gospodarczych nie mają żadnych zabezpieczeń, (np. przeciwpożarowych) lub te, które posiadają są nieodpowiednie dla rodzaju chronionego majątku. Taki widok budzi grozę. Zdarza się, że kierownictwa firm nie zdają sobie sprawy z braku dobrych zabezpieczeń i dopiero powstałe szkody weryfikują tę wiedzę. Zaistniałe zdarzenie spowodować może częściowe lub całkowite wstrzymanie procesów produkcyjnych. A przeciętnemu człowiekowi ujawni się to np. w momencie, gdy nie będzie mógł wypłacić pieniędzy z bankomatu lub nie będzie działała jego karta kredytowa. Otrzymany wówczas oficjalny komunikat potwierdzi zerwanie łączności ze źródłem przetwarzającym informacje.

Historia o tym, jak proszkiem gaszono serwery

Znany jest przypadek szkody, do której doszło kilka lat temu, a którą spowodowały niewłaściwie dobrane urządzenia gaśnicze. Zabezpieczyły one nowo zbudowaną serwerownię jednej z największych instytucji finansowych w kraju. W firmie tej, której działalność wspierana jest w znaczącej mierze przez systemy informatyczne, serwerownię - która



miała obsługiwać najważniejsze procesy - zabezpieczono bowiem stałymi urządzeniami gaśniczymi aerozolowymi, inaczej proszkowymi. Ich charakterystyczną cechą jest wytwarzanie wysokiej temperatury podczas działania, nawet rzędu kilkuset stopni. Dzięki temu możliwe jest wydostanie się - wskutek wybuchu materiału zapalającego - środka gaśniczego do chronionej atmosfery. Uruchamianie systemu odbywa się automatycznie, po „zauważeniu” dymu przez czujki.

Serwery nie były jeszcze włączone do systemu firmy. Trwało wgrzywanie programów „produkcyjnych”. Kwestią kilku dni była synchronizacja odpowiednich aplikacji. Serwery pracowały przez cały czas, oswajając się z wiedzą wpompowaną wcześniej w postaci programów. Pewnej nocy, w czasie weekendu, gdy w pomieszczeniu nie było nikogo, czujki wykryły dym, wydobywający się prawdopodobnie z tłącego się przewodu zasilającego sprzęt. Nastąpiło przekazanie sygnału do centralki obsługującej urządzenia gaśnicze, a następnie rozpoczęło się odliczanie. System gaśniczy skonfigurowano bowiem w taki sposób, by po wykryciu dymu przez czujki nie następowało natychmiastowe uruchamianie urządzeń. Czas zwłoki umożliwił ewakuację osób pracujących w pomieszczeniu, a ochroniarzom pozwalał na dotarcie do pomieszczenia i sprawdzenie, co się faktycznie stało. Przy drzwiach wejściowych zamontowany był przycisk pozwalający na wyłączenie systemu po stwierdzeniu fałszywego alarmu. Po upływie czasu przeznaczanego na sprawdzenie pomieszczenia (i ewentualną ewakuację), urządzenia gaśnicze uruchomiły się. Z agregatów wydostał się proszek, tworząc w powietrzu gęstą zawiesinę. Przy okazji - podczas wypierania środka gaśniczego z agregatów - temperatura w pomieszczeniu znacznie się podniosła. Po zakończeniu „akcji gaśniczej” pracownicy firmy, zwiedzając

pomieszczenie stwierdzili, że proszek spenetrował dokładnie wnętrza serwerów, czyniąc spustoszenia wszędzie tam, gdzie były elementy ruchome. Szczególnie dotyczyło to twardych dysków, które się „zatarły”. Temperatura w pomieszczeniu była tak wysoka, że czujniki temperatury zamontowane w serwerach odłączyły napięcie przy ok. 100°C.

Obrazowo, w pomieszczeniu tym, wyglądało jak w młynie, gdzie mąka sypie się na posadzkę, zamiast do worków. Wartość uszkodzonego sprzętu osiągnęła kwotę kilkunastu milionów złotych. Za szczęście w nieszczęściu można uznać fakt, że serwery nie były w pełni włączone w system przedsiębiorstwa. A gdyby opisane zdarzenie powstało w ciągu normalnego dnia pracy, w godzinach 10.00-15.00, w szczytowym okresie „produkcji” przedsiębiorstwa? Biorąc pod uwagę znaczący udział firmy w krajowym rynku usług finansowych, klienci - delikatnie rzecz ujmując - byłiby co najmniej rozczarowani. Tak poważne straty, związane z kilkugodzinną przerwą w podstawowej działalności przedsiębiorstwa, byłyby trudne do oszacowania. Można postawić pytanie: dlaczego zatem zdecydowano się na taki system? Odpowiedź leży jedynie w sferze domysłów, a żartobliwie rzecz ujmując, jak napisał Horacy „*Quandoque bonus dormitat Homerus*” (w wolnym tłumaczeniu: czasami i ludzie wielcy mają chwile słabości).

Kluczowe pytania

Aby uniknąć uszkodzeń lub poważnego zniszczenia sprzętu elektronicznego zainstalowanego w serwerowniach, sterowniach i nastawniach, należy wnikliwie rozważyć możliwe do zastosowania zabezpieczenia. Poniżej przedstawiona jest grupa zdarzeń, przed którymi może być chroniony sprzęt. Ograniczona została grupa zagrożeń

związanych z takim ryzykiem, jak pożar i szeroko rozumiane kradzieże (włamanie i wszelkie inne formy wandalizmu). Bardzo istotna jest również ocena wartości chronionego majątku oraz jego znaczenia dla organizmu firmy, czyli odpowiedzi na pytania:

- 1) Jaka jest wartość odtworzeniowa chronionego majątku, tzn. ile będzie kosztował zakup nowego sprzętu o takich samych parametrach?
- 2) Czy czynności i procesy realizowane przez ten majątek włączone są w zasadniczy „krwioobieg” przedsiębiorstwa?
- 3) Czy, w przypadku uszkodzenia lub zniszczenia tego majątku, przedsiębiorstwo będzie funkcjonowało bez większych zakłóceń i przerw?

Ocena taka jest niezbędna, by uniknąć sytuacji, w której cena montażu systemów zabezpieczających przekraczałaby wartość i znaczenie chronionego majątku.

Pożar

Dla szacowania poziomu zagrożeń pożarowych potrzebne jest określenie prawdopodobnych, możliwych szkód. Duże zagrożenie pożarem stwarzają, między innymi, tworzywa sztuczne stanowiące element izolacji przewodów, kabli, płytek drukowanych. Nie bez wpływu na wzrost zagrożenia pozostaje np. składowanie w opisywanych, newralgicznych pomieszczeniach papieru - na przykład pustych kartonów po sprzęcie czy dokumentów.

ZABEZPIECZENIA KONSTRUKCYJNE

Pierwsza podstawowa zasada: pożar z zewnątrz nie może przenieść się do pomieszczenia ze sprzętem elektronicznym. Dlatego też ściany i drzwi muszą posiadać odpowiednią klasę odporności ogniowej, zapewniającą przez określony czas nieprzenikanie powstających podczas pożaru: energii cieplnej i dymu. Wszelkie przejścia przewodów przez ściany także muszą być odpowiednio uszczelnione (muszą posiadać tę samą odporność ogniową, co ściana).

Dotychczas znane są dwa przypadki z elektrowni krajowych, gdy pożar z sąsiadujących pomieszczeń, przeniósł się przez nieszczelne otwory w ścianach i stropach do wnętrza nastawni (pomieszczenie, z którego steruje się pracą kotła i turbozespołu wytwarzającego energię elektryczną). Efektem było całkowite jej zniszczenie i jednoczesne wstrzymanie pracy obsługiwanych bloków energetycznych. Słowem - nastąpiła przerwa w produkcji energii elektrycznej.

Wracając do zabezpieczeń konstrukcyjnych, zgodnie z warunkami amerykańskiej normy NFPA 75 ściany i drzwi serwerowni, sterowni oraz wszelkich podobnych pomieszczeń powinny posiadać minimalną klasę odporności ogniowej na poziomie 60 minut.

Dla lepszego wyobrażenia działania temperatury i wilgoci na sprzęt elektroniczny warto przytoczyć graniczne wielkości tych parametrów, przy których już następuje uszkodzenie sprzętu:

- temperatura ok. 66°C:

wg NFPA 75 Standard for the Protection of Electronic Computer/Data Processing Equipment Protection Standard, 2003 Edition,

- temperatura ok. 70°C i wilgotność ok. 85%:

wg norm europejskich - EN1047, dla infrastruktury informatycznej - test według normy DIN 4102 F 90.

Znając wartość sprzętu, jego znaczenie dla firmy oraz wielkość temperatury, przy której następuje uszkodzenie sprzętu, wypada zastanowić się nad tym, jakie zabezpieczenia (i czy w ogóle) można stosować, aby go jak najlepiej chronić.

Upraszczając, w ocenie technicznej ryzyka, zabezpieczenia dzielimy na: konstrukcyjne, techniczne, organizacyjne. Przepisy państwowe w niewielkim zakresie stawiają wymagania pomieszczeniom ze sprzętem elektronicznym o znacznej wartości. Jedynie Rozporządzenie MSWiA z 16 czerwca 2003 roku (Dz. U. nr 121, poz. 1138) wspomina o tym problemie i to dość powierzchownie.

Wszelkie, poniżej opisane rozważania, opierają się na stosowanych standardach światowych oraz na powszechnie znanych zasadach tzw. dobrej praktyki technicznej.

Oznacza to, że wykonać je należy z takich materiałów, aby promieniowanie cieplne i produkty spalania w czasie 60 minut w warunkach normowych (badawczych) nie mogły przez nie przechodzić i zapewniły pełną izolację. Inne wymagania stawiane przez największe firmy reasekuracyjne określają, że ściany serwerowni powinny być wykonane z żelbetonu o grubości minimum 10 cm. Kolejnym zabezpieczeniem przed rozprzestrzenieniem się ognia z sąsiednich pomieszczeń, jest montaż kłap przeciwpożarowych w kanałach wentylacyjnych.

Gdyby we wspomnianych elektrowniach nastawnie posiadały odpowiednie zabezpieczenia konstrukcyjne, a przynajmniej przejścia kabli i przewodów przez ściany i stropy byłyby właściwie uszczelnione, nie doszłoby do ich całkowitego zniszczenia i co za tym idzie, elektrownie pracowałyby bez większych problemów. Straty samego zniszczonego i uszkodzonego majątku opiewały na kwotę kilkudziesięciu milionów złotych.

Na jaką kwotę wycenić można by wykonanie właściwych zabezpieczeń otworów w ścianach wymienionych nastawni? Może dwa, trzy, cztery, a maksymalnie do pięciu tysięcy złotych? Taka kwota to zaledwie ułamek środków finansowych, które pochłonęła odbudowa i odtworzenie wyposażenia nastawni.

W krajowych elektrowniach, w ciągu ostatnich dziesięciu lat, przeprowadzono znaczące modernizacje, które obejmowały przede wszystkim urządzenia wytwórcze - turbozespoły i kotły. Efektem tego, było wprowadzanie na szeroką skalę automatyki pomiarowej i systemowej, w oparciu o cyfrowe przetwarzanie danych, skupione w nastawniach.

W większości przypadków, po modernizacji, pomieszczenia nastawni pozostawały na dotychczasowym miejscu w budynku głównym, w pobliżu turbozespołów, gdzie poważne zagrożenie pożarem stwarza zgromadzony w ogromnych ilościach (przynajmniej kilkadziesiąt ton na jeden turbozespół) olej, niezbędny do celów technologicznych.

W pomieszczeniach nastawni zamontowano sprzęt komputerowy do sterowania i analizowania pracy zainstalowanych urządzeń. Brak poprawy bezpieczeństwa konstrukcyjnego pomieszczeń nastawni, to nie tylko wspomniane już otwory na przejścia instalacji przez ściany i stropy, ale także okna wychodzące do maszynowni, gdzie stosowany jest olej - okna posiadają szyby zwykłe, bezklasowe z punktu widzenia bezpieczeństwa pożarowego.

Zdarza się, że drzwi prowadzące z maszynowni do nastawni są również „zwykłe”, czyli niezapewniające odpowiedniej odporności ogniowej. Zgromadzony za nimi



majątek, którego wartość szacowana jest średnio na kilkanaście do kilkudziesięciu milionów złotych, ma żywotne znaczenie dla elektrowni. Dla porównania sytuacji - wyobraźmy sobie serwerownię banku, w którym posiadamy rachunek osobisty. Serwerownia obsługująca nasze karty płatnicze przez szybę sąsiaduje z przepompownią paliw. Dodatkowo przepompowywanie odbywa się w sąsiedztwie rurociągów, nagranych do temperatury kilkuset stopni Celsjusza, a każdy wyciek paliwa z instalacji spowoduje pożar.

Skąd zatem taka, rzec można, niefrasobliwość w zabezpieczaniu wspomnianych nastawni? Zapewne wynika ona z przywiązania niektórych menedżerów IT jedynie do wymagań przepisów państwowych, bez uwzględniania specyfiki branży.

Jeżeli, zgodnie z krajowymi przepisami, nie ma konieczności odpowiedniego wydzielenia przeciwpożarowego nastawni od maszynowni, to kwestia ta nie jest przedmiotem szczególnych analiz, a zakres modernizacji pomieszczenia sprowadza się do wyrównania podłogi i pomalowania ścian oraz wymiany szyb na nowe w przypadku, gdy stare były popękane.

Ile kosztowałyby odpowiednie wydzielenie przeciwpożarowe nastawni? Maksymalnie od kilkunastu do kilkudziesięciu tysięcy złotych, czyli nieporównywalnie mało z całkowitą modernizacją bloku rzędu minimum kilkudziesięciu milionów złotych.

ZABEZPIECZENIA TECHNICZNE

Ten rodzaj zabezpieczeń obejmuje sygnalizację pożarową i urządzenia gaśnicze.

Sygnalizacja pożarowa w opisywanych pomieszczeniach opierać się może na „tradycyjnych” czujkach dymu. Jednak należy zwrócić uwagę na ciągłą cyrkulację powietrza w typowej serwerowni, związanej z koniecznością chłodzenia dysków i procesorów. Krążące w pomieszczeniu powietrze, w znacznym stopniu może rozrzedzać dym i jego w miarę szybkie „zauważenie” przez „tradycyjnie” stosowane czujki może zostać opóźnione.

Dlatego bardziej zaawansowane systemy sygnalizacji analizują w sposób ciągły skład powietrza i mogą wykryć najmniejsze części, znajdującego się w nim dymu. Ich działanie polega na zasysaniu powietrza zarówno z szaf serwerów, jak i z całego pomieszczenia. Alarmowanie, czyli informowanie o wykryciu pożaru oraz uruchomienie - przykładowo - urządzeń gaśniczych, jest kwestią odpowiedniej konfiguracji całego systemu, zarówno dla sygnalizacji na bazie czujek „tradycyjnych”, jak i urządzeń zasysających.

Następna grupa zabezpieczeń technicznych to stałe urządzenia gaśnicze. Podstawowym warunkiem, jaki musi zostać spełniony przy

wyborze środka gaśniczego jest brak cech fizycznych i chemicznych negatywnie oddziałujących na chroniony majątek. Inaczej rzecz ujmując, zastosowany do gaszenia sprzętu elektronicznego środek gaśniczy nie może zniszczyć, a nawet uszkodzić zabezpieczanych urządzeń.

Wyobraźmy sobie polewanie wodą płonącego komputera lub użycie proszku gaśniczego. Zarówno w pierwszym, jak i w drugim przypadku, skutkiem akcji gaśniczej będzie zniszczenie sprzętu. Istotą możliwych do zastosowania środków gaśniczych musi być obniżenie, przez określony czas (właściwy dla danego środka gaśniczego), stężenia tlenu do poziomu około 13-14 procent, przy którym to proces spalania zostanie przerwany.

Dlaczego sprawa utrzymywania stężenia środka gaśniczego przez określony czas jest tak istotna? Obowiązujące normy zakładają, że - przykładowo - centrale telefoniczne lub inne ważne serwerownie w czasie pożaru będą pracowały w systemie ciągłym, stanowiąc tym samym potencjalne źródło pożaru wtórnego, zaś utrzymanie obniżonej zawartości tlenu ma takiemu pożarowi zapobiec.

Kolejnymi ważnymi cechami środków gaśniczych są również: efekt fizycznego pochłaniania ciepła i chemicznego oddziaływania na płomień.

Dotychczas do ochrony sprzętu elektronicznego powszechnie stosowano halony - środki gaśnicze oparte na związkach chloru, fluoru, bromu lub jodu. Istotą ich działania jest wchodzenie w reakcję z płomieniem. Skuteczność tych środków jest bardzo wysoka, jednak posiadają negatywną cechę - pochłaniają ozon zawarty w atmosferze, przyczyniając się do wzrostu efektu cieplarnianego. Polska w 1990 roku podpisała - podobnie jak inne kraje - Protokół Montrealski i zobowiązała się do wycofania halonów.

Zostały one zastąpione przez chlorowcopochodne, tzw. zamienniki halonów - posiadające jednak sporo cech wspólnych z halonami - oraz gazy obojętne tj. środki zawierające, jako główny składnik, jeden lub więcej gazów takich, jak: hel, neon, argon lub azot. Składnikiem dodatkowym gazów obojętnych może być dwutlenek węgla. Przy projektowaniu stałych urządzeń gaśniczych wykorzystuje się doświadczenia zawarte w normach:

- ISO 14520: 1-15 Gaseous fire - extinguishing systems - Physical properties and system design,
- NFPA 2001 Standard on Clean Agent Fire Extinguishing Systems 2000 Edition.

Dysze, z których wydobywa się gaz gaśniczy mogą znajdować się bezpośrednio w pomieszczeniu, jak i pod podniesioną podłogą oraz ponad podwieszonym sufitem.

Dodatkowo, w celu uniknięcia zniszczenia sprzętu komputerowego wskutek nadmiernego wzrostu ciśnienia, w pomieszczeniu montuje się klapy odciążające, które „wyprowadzają” część ciśnienia na zewnątrz.

Jak już wspomniano, najważniejszą cechą stosowanych środków gaśniczych powinno być niedoprowadzenie do uszkodzenia lub zniszczenia sprzętu elektronicznego. Powracając zatem do opisanego wcześniej przypadku pożaru w serwerowni zabezpieczonej stałymi urządzeniami gaśniczymi aerozolowymi, inaczej proszkowymi, należy z całą stanowczością podkreślić, że zastosowanie proszku - substancji bardziej rozdrobnionej niż mąka - do gaszenia komputerów i wszelkiego rodzaju sprzętu elektronicznego jest niewłaściwe.

Wielokrotnie w odwiedzanych serwerowniach, można było zauważyć gaśnice proszkowe stojące w pobliżu drzwi, służące do gaszenia pożarów typu A, B, C (A - ciała stałe pochodzenia organicznego, tj. drewno, papier, tworzywa sztuczne itp.; B - ciecze palne; C - gazy palne). Na pytanie o to, kto polecił postawienie takiej gaśnicy akurat w takim miejscu, z reguły pada odpowiedź - „strażak”. Przekazanie osobie obsługującej sprzęt elektroniczny, przeważnie informatykowi, szczegółowych informacji o zasadach działania proszku gaśniczego, powodowało zrozumienie niszczylińskiego jego działania. Nie skutkowało jednak zmianą środka gaśniczego.

Biorąc pod uwagę znaczne koszty zainstalowania stałych urządzeń gaśniczych, należy rozważyć, jakie techniczne zabezpieczenia przeciwpożarowe można stosować w mniejszych serwerowniach lub w pomieszczeniach ze sprzętem elektronicznym o mniejszej wartości i znaczeniu, w których montaż stałych urządzeń gaśniczych jest nieuzasadniony z ekonomicznego punktu widzenia.

Na rynku polskim pojawiły się już gaśnice zawierające chlorowcopochodne. Istnieją też gaśnice z dwutlenkiem węgla. Przed jego użyciem należy jednak uwzględnić, co może się stać, jeśli gaz schłodzony do temperatury kilkunastu stopni Celsjusza poniżej zera dostanie się na rozgrzane elementy komputera, a w szczególności na gniazda zaciskowe procesora. Nastąpi wówczas skroplenie wody z powietrza, co doprowadzić może do zwarcia na zaciskach, a w dalszej konsekwencji do uszkodzenia procesora.

Reasumując, tam gdzie jest to konieczne, należy stosować stałe urządzenia gaśnicze, bazujące najlepiej na gazach obojętnych lub na chlorowcopochodnych. Natomiast tam, gdzie nie jest to ekonomicznie uzasadnione, powinno stosować się gaśnice zawierające chlorowcopochodne. W ostateczności można umieścić gaśnice z dwutlenkiem węgla.

ZABEZPIECZENIA ORGANIZACYJNE

Zabezpieczenia organizacyjne to przede wszystkim znajomość zasad działania systemów bezpieczeństwa przez obsługę i ochronę. Czynnikiem ludzki niejednokrotnie jest najsłabszym ogniwem całego systemu szeroko rozumianego bezpieczeństwa.

Wielokrotnie można spotkać w różnych firmach ochroniarzy, którzy nie mają podstawowego pojęcia o obsłudze urządzeń przeciwpożarowych i przeciwkradzieżowych.

Zdarza się, że problemem jest zwykle alarmowanie, za pomocą telefonów, straży pożarnej lub policji. Bywa i tak, że ochroniarze strzegący wielomilionowych majątków przychodzą do pracy, aby wypocząć. Sytuacje takie zdarzają się jednak coraz rzadziej - rosną wymagania oraz nadzór ze strony właścicieli firm.

Aspekty organizacyjne, związane z bezpieczeństwem, to także utrzymywanie odpowiedniego poziomu porządku w omawianych pomieszczeniach. Nierzadko serwerownia służy jako skład pustych kartonów i zbędnego papieru lub archiwum dokumentów. Wszechobecne kosze na śmieci z tworzyw sztucznych stały się, w pewnym momencie, standardem.

Dla poprawy stanu bezpieczeństwa, w pomieszczeniach ze sprzętem elektronicznym o znacznej wartości i znaczeniu, zaleca się:

- nie gromadzić zbędnych materiałów palnych w postaci kartonów, dokumentów itp.,
- stosować jedynie metalowe kosze na śmieci i systematycznie je opróżniać,
- nie składować zbędnych kabli i przewodów, mających służyć do budowy sieci.

KRADZIEŻE

Jak należy zabezpieczyć pomieszczenie przed dostępem osób postronnych? Ponownie należy postawić pytania dotyczące wartości chronionego sprzętu, jego znaczenia oraz sposobu obsługi. Na przykład - czy w pomieszczeniu stale przebywają ludzie? Dzieje się tak chociażby we wszelkiego rodzaju nastawniach i sterowniach, w których stała obecność ludzi wiąże się z operacjami technologicznymi.

TELEWIZJA PRZEMYSŁOWA

W kraju i na świecie rośnie znaczenie telewizji przemysłowej. Ukryte kamery rejestrują nas, gdy dokonujemy zakupów w różnego rodzaju sklepach, począwszy od tych największych, a na najmniejszych, osiedlowych, skończywszy. Podobnie sprawa wygląda w pomieszczeniach ze sprzętem elektronicznym. Zaleca się stosowanie telewizji



przemysłowej szczególnie w serwerowniach oraz we wszelkiego rodzaju nastawniach i sterowniach. Wszędzie tam można odtworzyć zarejestrowany obraz i dowiedzieć się, kto, jak długo i co robił w danym pomieszczeniu. Najlepszą jakością obrazu zapewniają nagrania dokonane w systemie cyfrowym.

Równie istotnym elementem jest przechowywanie nagranych obrazów a w szczególności czas i warunki przechowywania. Zarówno w zakresie czasu, jak i warunków przechowywania nagrań, brak jest polskich przepisów. Praktyka wskazuje, że wystarczającym okresem przechowywania zarejestrowanego obrazu jest trzydzieści dni. Nośniki z nagraniami powinny być składowane w odpowiednio zabezpieczonym, pod względem przeciwpożarowym i antywłamaniowym, miejscu.

DOSTĘP DO POMIESZCZEŃ

Wejście do pomieszczeń ze sprzętem elektronicznym, a szczególnie do serwerowni, powinno być ograniczone do wybranych osób. Kontrolę dostępu można realizować za pomocą wszelkiego rodzaju czytników: kart magnetycznych, skanerów linii papilarnych i siatek oczu.

Co wydaje się jednak najważniejsze z punktu widzenia bezpieczeństwa? Czytniki powinny znajdować się zarówno na zewnątrz pomieszczenia, jak i wewnątrz. Każdorazowe otwieranie drzwi (przy wchodzeniu i wychodzeniu), szczególnie serwerowni, gdzie osoby przebywają sporadycznie, będzie wówczas możliwe jedynie z użyciem czytnika. Dzięki takiemu rozwiązaniu można dokładnie odtworzyć, kto i jak długo przebywał w środku. Jest to szczególnie ważne przy dochodzeniu przyczyny szkody i ustalaniu jej sprawcy.

ELEKTRONICZNE SYSTEMY WŁAMANIA

Do elektronicznych systemów włamania zalicza się szeroką gamę czujek ruchu, stłuczenia szyb, barier podczerwieni itp. Zastosowanie określonego urządzenia zależy od dokładnej analizy występujących zagrożeń.

Praca systemu powinna być komputerowo rejestrowana, aby można było dokładnie określić poszczególne stany jego pracy, np. uruchomienie czujek, przyjazd patrolu firmy ochroniarskiej.

INTEGRACJA SYSTEMÓW

Nie można zapomnieć o integracji systemów, tj. konfiguracji poszczególnych, wymienionych powyżej elementów (telewizji przemysłowej, kontroli dostępu, systemów antywłamaniowych), w taki sposób, aby zapewnić maksymalną jego efektywność. Na przykład czujka ruchu może uruchamiać ciągłą rejestrację obrazu przez kamery telewizji przemysłowej z jednoczesnym wysłaniem sygnału do firmy ochroniarskiej.

Zasadność zastosowania powyższych zabezpieczeń przeciwkradzieżowych dotyczy również pomieszczeń ze sprzętem elektronicznym o mniejszej wartości.

Zaistniałe szkody pokazują, że np. wartość utraconego laptopa, nieistotna z punktu widzenia firmy, jest niewspółmierna do wartości utraconych danych, zapisanych na jego twardym dysku.

Niektóre z rozważań, dotyczących zagadnień organizacyjnych, wspomnianych przy omawianiu pożarów, odnoszą się także do ryzyka włamań.

W niniejszym artykule wspomniano jedynie o najistotniejszych kwestiach i problemach zabezpieczeń związanych z ochroną przeciwpożarową i przeciwkradzieżową. Odrębnymi rozważaniami należy objąć zagadnienia dotyczące zabezpieczeń przepięciowych, odgromowych, antyzalaniowych i innych.

Przyszłość - rosnące znaczenie pomieszczeń kluczowych

Wszechobecność informatyki i internetu jest dzisiaj niepodważalnym faktem. Gordon Moore jeden z założycieli Intel'a w 1965 roku stwierdził, że liczba tranzystorów w chipie będzie podwajała się co 12 miesięcy. Opinia ta została zweryfikowana już w połowie lat siedemdziesiątych ubiegłego wieku. Od tego czasu szybkość działania komputerów podwaja się co 18 miesięcy. Niesie to za sobą dynamiczny rozwój technologii, napędzających każdą działalność człowieka. Wraz z tym, rośnie liczba pomieszczeń, a nawet całych obiektów, w których znajduje się sprzęt elektroniczny, służący do przetwarzania niezliczonych ilości danych. Ich znaczenie dla funkcjonowania przedsiębiorstw idąc dalej, całej gospodarki - również wzrasta w sprinterskim wprost tempie.

Krzysztof Kowalczyk
krzysztof.kowalczyk@hestia.pl

