Bezpieczeństwo IT w firmie

IT Omega Sp. z o.o.
z siedzibą al. Solidarności 117
00-140 Warszawa

Oddział I:
al. Jana Pawła II 45A
01-008 Warszawa

Kontakt
infolinia: (22) 3 500 800
e-mail: obsluga@itomega.pl

W PORADNIKU

- Ochrona danych
- Oprogramowanie antywirusowe
- Zabezpieczenie serwerów
- Bezpieczeństwo sieci
- Umowa SLA

IT Omega Sp. z o.o.
z siedzibą al. Solidarności 117
00-140 Warszawa

Oddział I:
al. Jana Pawła II 45A
01-008 Warszawa

Kontakt
infolinia: (22) 3 500 800
e-mail: obsluga@itomega.pl

Przedsiębiorstwa wytwarzają i przetwarzają w sieci coraz więcej danych.

Według szacunków firmy badawczej IDC na przestrzeni ostatnich lat liczba informacji wzrosła pięciokrotnie.

Firmy dostrzegają konieczność inwestowania w system zabezpieczenia danych nie tylko na komputerach pracowników ale również na serwerach. Nie bez znaczenia jest również ochrona sieci oraz danych w przypadku fizycznego uszkodzenia nośnika.

Tomasz Janas
CEO IT Omega Sp z o.o.

Aby nie narazić przedsiębiorstwa na straty należy skorzystać z doświadczenia firm specjalizujących się w zabezpieczaniu systemów informatycznych. Przełoży się to na wybór rozwiązań z zakresu bezpieczeństwa IT optymalnych pod kątem kosztów jak i właściwie zabezpieczających firmowe zasoby.

IT Omega Sp. z o.o.
z siedzibą al. Solidarności 117
00-140 Warszawa

Oddział I:
al. Jana Pawła II 45A
01-008 Warszawa

Kontakt
infolinia: (22) 3 500 800
e-mail: obsluga@itomega.pl

Awarie i utrata danych w firmie. Jak ich uniknąć?

Uszkodzenie sprzętu, źródła zasilania, nośników, wadliwie działające programy - to czynniki najczęściej wymieniane w przypadku utraty danych. Według badania przeprowadzonego przez Kaspersky Lab i B2B International, najpowszechniejszym zagrożeniem wewnętrznym nadal są luki w zabezpieczeniach oprogramowania - wskazane przez 32 proc. badanych firm europejskich. W dalszej kolejności wskazano przypadkowy wyciek danych spowodowany przez personel (26 proc. badanych firm) oraz utratę urządzeń mobilnych przez personel na skutek zgubienia lub kradzieży (29 proc. respondentów). Jako główne przyczyny utraty danych w wyniku incydentów wewnętrznych 15 proc. firm wskazało incydent, w którym wykorzystano lukę w oprogramowaniu, 18 proc. przyznało się do utraty danych na skutek przypadkowego wycieku spowodowanego przez personel.

W ciągu 2 lat o 12 proc. spadnie liczba przedsiębiorców przechowujących kopie zapasowe danych we własnej lokalizacji.

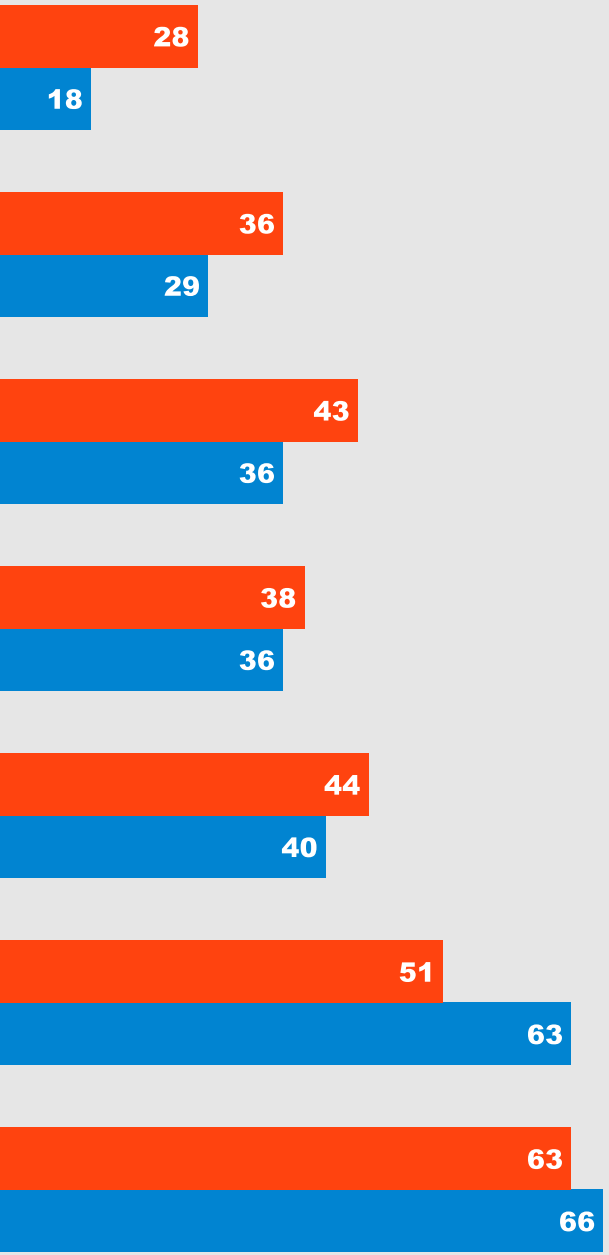
IT Omega Sp. z o.o.
z siedzibą al. Solidarności 117
00-140 Warszawa

Oddział I:
al. Jana Pawła II 45A
01-008 Warszawa

Kontakt
infolinia: (22) 3 500 800
e-mail: obsluga@itomega.pl

Z jakich metod ochrony danych i odzyskiwania po awarii przedsiębiorstwo korzysta obecnie i zamierza korzystać za dwa lata?

źródło: 2016 Veeam Availability Report



TECHNOLOGIA	PLANY NA 2018
Migawki pamięci masowej w dodatkowej pamięci zewnętrznej	↑ + 10 proc.
Migawki pamięci masowej w dodatkowej pamięci lokalnej	↑ + 7 proc.
Replikacja w lokalizacji zewnętrznej	↑ + 7 proc.
Migawki pamięci masowej	↑ + 2 proc.
Replikacja lokalna	↑ + 4 proc.
Lokalne kopie zapasowe	↓ - 12 proc.
Kopie w lokalizacji zewnętrznej (dysk, taśma, chmura)	↓ - 3 proc.

Korzysta obecnie
Zamierza korzystać za 2 lata

Backup, czyli...

...proces kopiowania danych w bezpieczne miejsce, to odpowiedź na te zagrożenia. Proces ten pozwala przedsiębiorstwom wyeliminować straty związane z utratą danych.

Na środowisko backupowe składają się sprzęt komputerowy, i oprogramowanie. Ich zadaniem jest efektywne zarządzanie kopiami danych oraz zabezpieczanie ich krótko i długotrwale.

„Serwer w firmie zawiera najcenniejsze aktywa - najważniejsze dane gromadzone przez lata w formie elektronicznej. Ich utrata wiąże się z realnymi stratami finansowymi. Zabezpieczenie serwerów naszych Klientów ma dla nas najwyższy priorytet. Rekomendowane przez nas oprogramowanie pozwala skrócić czas odzyskiwania danych po awarii serwera z kilku dni roboczych do 2 godzin". – mówi Tomasz Janas CEO IT Omega Sp z o.o.

IT Omega Sp. z o.o.
z siedzibą al. Solidarności 117
00-140 Warszawa

Oddział I:
al. Jana Pawła II 45A
01-008 Warszawa

Kontakt
infolinia: (22) 3 500 800
e-mail: obsluga@itomega.pl

Przypadki utraty danych

źródło: Kroll Ontrack

01 ATAK HACKERÓW

Utrata danych nierzadko bywa wywołana celowym działaniem. W Stanach Zjednoczonych grupa hakerów zaatakowała pewien hotel i usunęła dane oraz kopie zapasowe z 35 dysków LUN.

Szkoda okazała się jednak odwracalna. Zespół specjalistów pracujących zarówno na miejscu, jak i zdalnie, odzyskał wszystkie utracone w wyniku ataku dane.

02 ZALANY SERWER

Powódź, jaka nawiedziła Bałkany w 2014 roku sprawiła, że pewien serwer RAID przedryfował niemal 100 metrów od miejsca, w którym pierwotnie się znajdował.

Poszukiwania urządzenia trwały dwa tygodnie.

Przez cały ten czas serwer znajdował się w wodzie. Na szczęście specjaliści odzyskali wszystkie zgromadzone na nim informacje.

03 SIECIOWA INTRYGA

Specjaliści zostali poproszeni o interwencję w sprawie pięcioletniego serwera, który dotknęła awaria. Kiedy inżynier otworzył serwer, znalazł w nim gniazdo pełne pająków. Kolejni „dzicy lokatorzy" zostali znalezieni w okolicach głowic jednego z dysków.

Snuta przez nich „sieciowa intryga" jednak się nie udała – odzyskano sto procent danych.

04 OSKAR DLA...

Podczas produkcji filmu niespodziewane wydarzenie stało się udziałem ekipy filmowej. Kiedy jej członkowie kopiowali dane, jeden z nich przypadkowo kopnął w stół. Zarówno laptop jak i dysk upadły na ziemię, niwecząc efekty 18-miesięcznej pracy 150-osobowego zespołu.

Udało się odzyskać ponad 80 procent utraconego materiału

IT Omega Sp. z o.o.
z siedzibą al. Solidarności 117
00-140 Warszawa

Oddział I:
al. Jana Pawła II 45A
01-008 Warszawa

Kontakt
infolinia: (22) 3 500 800
e-mail: obsluga@itomega.pl

OPROGRAMOWANIE ANTYWIRUSOWE

Czy firma musi posiadać oprogramowanie antywirusowe?

Według rozporządzenia MSWiA (Dz. U. z 2004 r. Nr 100, poz. 1024) w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych znajdziemy zapis stanowiący: **System informatyczny, służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed: działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.**

Warto zwrócić uwagę, że obecnie praktycznie każde przedsiębiorstwo gromadzi i przetwarza dane osobowe. Co więcej stropień ochrony jaki musimy zapewnić w naszej firmie według wspomnianego wyżej rozporządzenia musi być **wysoki**.

Poziom wysoki stosuje się, gdy przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest siecią publiczną.

IT Omega Sp. z o.o.
z siedzibą al. Solidarności 117
00-140 Warszawa

Oddział I:
al. Jana Pawła II 45A
01-008 Warszawa

Kontakt
infolinia: (22) 3 500 800
e-mail: obsluga@itomega.pl

Odpowiedź na pytanie czy firma musi inwestować w ochronę antywirusową stanowisk swoich pracowników brzmi: tak.

Co więcej według prawa musi być to ochrona na najwyższym z możliwych poziomów.

Antywirus

Systemy antywirusowe stanowią ochronę naszych urządzeń przed atakami i następstwami działania wirusów oraz robaków. Brak zabezpieczeń przed ich działaniem może zakończyć się nieodwracalnymi stratami. Podstawowym narzędziem, które możemy wykorzystać do ochrony jest oprogramowanie antywirusowe. Oprogramowania te zainstalowane na wszystkich serwerach oraz stacjach roboczych prowadzą nieustanny monitoring. Sprawdzają ruch sieciowy oraz pliki jakie uruchamiamy na naszych komputerach.

ZABEZPIECZENIE SERWERÓW

Na czym polega utwardzanie zabezpieczeń?

Na utwardzanie systemów (tzw. hardening) składa się szereg działań, których celem jest optymalizacja i poprawa zabezpieczeń systemów operacyjnych serwerów oraz urządzeń końcowych pracujących w infrastrukturze IT.

Tak przygotowane środowisko jest podstawą do stabilnej pracy oraz zapewnienia ciągłości procesów biznesowych Klientów. Istotnym aspektem jest również zapewnienie ochrony przed atakami DDoS - mające na celu zatrzymanie infrastruktury IT.

Tomasz Janas
CEO IT Omega Sp z o.o.

Proces utwardzania polega na odpowiedniej konfiguracji wszystkich elementów systemu, zaczynając od logowania, usług sieciowych, zasobów udostępnianych na odpowiedniej konfiguracji kart sieciowych kończąc. Podejmowane w ramach „utwardzania" czynności skutecznie zabezpieczają serwery przed włamaniami.

IT Omega Sp. z o.o.
z siedzibą al. Solidarności 117
00-140 Warszawa

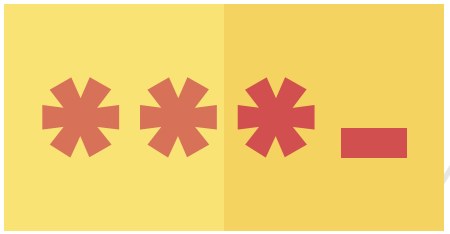
Oddział I:
al. Jana Pawła II 45A
01-008 Warszawa

Kontakt
infolinia: (22) 3 500 800
e-mail: obsluga@itomega.pl

Rozkład liczby ataków DDoS według dnia tygodnia

źródło: Kaspersky Lab

W II kwartale najaktywniejszym dniem tygodnia jeśli chodzi o ataki DDoS był wtorek. Najspokojniejszym dniem tygodnia pod względem ataków DDoS okazała się niedziela.



Ile kosztuje przeprowadzenie ataku DDoS na stronę internetową?

Jest to kwota od kilku do kilku tysięcy dol.!

Wiele firm zdejmuje swoje strony internetowe z sieci do czasu,gdy atak się skończy.

IT Omega Sp. z o.o.
z siedzibą al. Solidarności 117
00-140 Warszawa

Oddział I:
al. Jana Pawła II 45A
01-008 Warszawa

Kontakt
infolinia: (22) 3 500 800
e-mail: obsluga@itomega.pl

W II kwartale 2016 r. dwie firmy - CoinWallet i Coinkite – poinformowały o zakończeniu swojej działalności na skutek długotrwałych ataków DDoS.

DDoS

„Niebezpiecznie jest traktować ataki DDoS jako zdarzenia, które występują rzadko, mogą przytrafić się firmie jednorazowo, przez przypadek, i powodują minimalne szkody. Z reguły jeśli atak się powiedzie, przestępcy ponownie wykorzystają to narzędzie przeciwko firmie, blokując jej zasoby przez dłuższy czas. Niestety, nawet jeden atak może spowodować duże straty finansowe i wizerunkowe, a zważywszy na to, że prawdopodobieństwo kolejnego ataku wynosi prawie 80 proc. Dla współczesnej firmy rozwiązanie zabezpieczające przed atakami DDoS jest tak samo potrzebne jak podstawowa ochrona przed szkodliwym oprogramowaniem oraz phishingiem". - powiedział Aleksiej Kisielew, menedżer projektu w zespole odpowiedzialnym za rozwiązanie Kaspersky DDoS Protection.

Ataki DDoS - mające na celu zatrzymanie infrastruktury IT - dotknęły jedną na sześć firm w okresie 12 miesięcy. Najbardziej ucierpiała branża budowlana, firmy IT oraz serwisy telekomunikacyjne. Większość firm (79 proc.) przyznała, że została zaatakowana więcej niż jeden raz, natomiast **niemal połowa firm padła ofiarą ataku czterokrotnie lub więcej razy.**

IT Omega Sp. z o.o.
z siedzibą al. Solidarności 117
00-140 Warszawa

Oddział I:
al. Jana Pawła II 45A
01-008 Warszawa

Kontakt
infolinia: (22) 3 500 800
e-mail: obsluga@itomega.pl

BEZPIECZEŃSTWO SIECI

Ochrona sieci za pomocą jednego urządzenia?

Ataki na firmy wyróżnia nie tylko częstotliwość, ale również czas trwania: 39 proc. ataków trwało krótko, natomiast 21 proc. badanych firm wskazało, że ataki, jakich doświadczyły, trwały kilka dni, czy nawet tygodni. Jeśli chodzi o szkody na reputacji, sytuację pogarsza dodatkowo sytuacja, w której firmy odkrywają, że zostały zaatakowane, dopiero gdy zostaną poinformowane o tym przez strony zewnętrzne.

Cyberprzestępcy zwykle atakują zasoby dostępne w internecie, takie jak:

- portale dla klientów (40 proc.)
- usługi komunikacyjne (40 proc.)
- oraz strony internetowe (39 proc.).

W takiej sytuacji klienci mogą jako pierwsi zauważyć, że serwis online działa nieprawidłowo. Niestety zabezpieczenie w postaci tradycyjnego firewalla przestaje już wystarczać.

79 proc. firm przyznało, że została zaatakowana więcej niż jeden raz, natomiast niemal połowa firm padła ofiarą ataku czterokrotnie lub więcej razy.

IT Omega Sp. z o.o.
z siedzibą al. Solidarności 117
00-140 Warszawa

Oddział I:
al. Jana Pawła II 45A
01-008 Warszawa

Kontakt
infolinia: (22) 3 500 800
e-mail: obsluga@itomega.pl

Ochrona sieci, stacji roboczych i użytkowników, zaawansowany router, koncentrator VPN – wszystko za pomocą jednego urządzenia?

„Od wielu lat implementujemy rozwiązania typu UTM (IDS/IPS). Jedno urządzenia spełnia wiele funkcji m.in. zaporę korporacyjną (firewall), wirtualne sieci prywatne (VPN), intrusion prevention system (IPS), ochronę antywirusową oraz antyspam, filtr adresów www i zaawansowane raportowanie".

Trwający 3 minuty atak o sile 5 Gbps, który można zlecić już za 5 dol., przekracza możliwości łącza większości firm w Polsce. Jedynie 30 dolarów kosztuje zlecenie ataku paraliżującego usługi internetowe dużego przedsiębiorstwa przez 2 godziny.

źródło: PAP

IT Omega Sp. z o.o.
z siedzibą al. Solidarności 117
00-140 Warszawa

Oddział I:
al. Jana Pawła II 45A
01-008 Warszawa

Kontakt
infolinia: (22) 3 500 800
e-mail: obsluga@itomega.pl

Unified Threat Management...

... to systemy które zapewniają zestaw wielu narzędzi zabezpieczających zintegrowanych w jedno urządzenie. W takim rozwiązaniu znajdziemy np. firewall, wraz z systemem antywirusowym, antyspamowym, systemem wykrywania i blokowania intruzów, którzy próbują wtargnąć do sieci, systemy kontrolowania treści oraz inne. Zastosowanie rozwiązań UTM wpływa znacząco na podniesienie bezpieczeństwa sieci, zasobów IT oraz aplikacji.

IDS/IPS

Intrusion Detection System i Intrusion Prevention System czyli systemy wykrywania i zapobiegania włamaniom do sieci. Systemy IDS/IPS są to urządzenia sieciowe zwiększające bezpieczeństwo sieci komputerowych przez wykrywanie (IDS) lub wykrywanie i blokowanie ataków (IPS) w czasie rzeczywistym. Systemy takie mogą pracować w kilku trybach w zależności od wybranego modelu sonda analizuje ruch i może go zablokować w razie wykrycia zagrożenia lub jeżeli nie wykryto żadnych nieprawidłowości ruch będzie przepuszczany.

UMOWA SLA

Co powinna zawierać umowa SLA?

W ramach SLA określane są parametry w zależności od zakresu usług. Parametry te powinny być definiowane w sposób jasny i pozwalający na ich weryfikację oraz odzwierciedlające potrzeby firmy. Dlatego też umowa SLA powinna być tworzona przez osoby mające odpowiednie doświadczenie.

Istotną częścią umowy SLA jest pakietu usług jakie otrzymuje Klient są to m.in.

- telefoniczne wsparcie techniczne,
- zagwarantowanie dostępności specjalistów reagujących na zgłoszone awarie,
- system rejestracji błędów,
- narzędzia do monitoringu dostępności usług.

SLA, czyli Service Level Agreement to umową między klientem a dostawcą usług określająca poziom i jakość świadczonych usług.

IT Omega Sp. z o.o.
z siedzibą al. Solidarności 117
00-140 Warszawa

Oddział I:
al. Jana Pawła II 45A
01-008 Warszawa

Kontakt
infolinia: (22) 3 500 800
e-mail: obsluga@itomega.pl

W umowie muszą się również znaleźć punkty zawierające:

- katalog usług świadczonych przez usługodawcę,
- wykaz parametrów jakościowych dla każdej z usług,
- rodzaje kar za niedotrzymanie parametrów jakości,
- sposób i zasady raportowania poziomu realizacji usług.

Warto również pamiętać o jednym z najczęściej popełnianych błędów podczas zawierania umowy SLA – zawyżonym poziomie dostępności i wsparcia systemu.

Wiele rozwiązań funkcjonujących w firmach działa w określonych godzinach, a ich brak dostępności w tym czasie powoduje znikome szkody. Dlatego parametr dostępności i czas wsparcia powinny być dobrane indywidualnie.

Przykładem takiego parametru może być żądanie dostępności usługi na poziomie 99,999 proc. w skali miesiąca.

Parametr dostępności usługi	
	Okres niedostępności (w skali miesiąca)
95 proc.	36 godzin
99 proc.	7 godzin
99,5 proc.	3 godziny
99,99 proc.	4 minuty
99,999 proc.	25 sekund
	Okres niedostępności (w skali roku)
95 proc.	18 dni 6 godzin
99 proc.	3 dni 15 godzin
99,5 proc.	1 dzień 19 godzin
99,99 proc.	50 minut
99,999 proc.	5 minut

IT Omega Sp. z o.o.
z siedzibą al. Solidarności 117
00-140 Warszawa

Oddział I:
al. Jana Pawła II 45A
01-008 Warszawa

Kontakt
infolinia: (22) 3 500 800
e-mail: obsluga@itomega.pl

Sieć komputerowa w firmie powinna być jak najlepiej zabezpieczona przed zagrożeniami pochodzącymi z Internetu. Nigdy nie jesteśmy w stanie zabezpieczyć się w 100 proc. jednak warto dopilnować, aby nasze zabezpieczenia były na tyle solidne, na ile możemy sobie pozwolić – począwszy od zabezpieczenia zgromadzonych, oprogramowanie antywirusowe do ochrony naszej sieci przed atakami. W przypadku kluczowych dla naszego biznesu usług warto zadbać o zabezpieczenie ich działania umową SLA.

IT Omega Sp. z o.o.
z siedzibą al. Solidarności 117
00-140 Warszawa

Oddział I:
al. Jana Pawła II 45A
01-008 Warszawa

Kontakt
infolinia: (22) 3 500 800
e-mail: obsluga@itomega.pl