Czy zarządzać bezpieczeństwem IT w urzędzie?

Główne ryzyka w zarządzaniu bezpieczeństwem IT

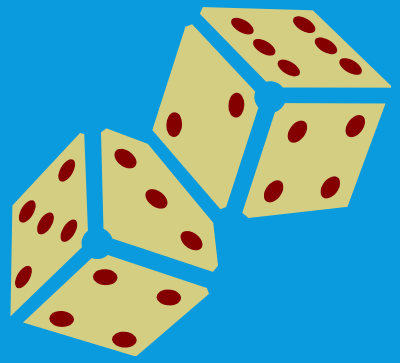
Damian Hoffman
Ekspert ds. bezpieczeństwa,
Instytut Prawa Nowych Technologii

email: damian@ipnt.pl

BEZPIECZEŃSTWO IT

Bezpieczeństwo IT - zbiór zagadnień z dziedziny telekomunikacji i informatyki związany z szacowaniem i kontrolą ryzyka wynikającego z korzystania z komputerów, sieci komputerowych i przesyłania danych do zdalnych lokalizacji.

Ryzyko - najogólniej, ryzyko jest wskaźnikiem stanu lub zdarzenia, które może prowadzić do strat. Jest ono proporcjonalne do prawdopodobieństwa wystąpienia tego zdarzenia i do wielkości strat, które może spowodować. Ryzyka nie da się wyeliminować i sprowadzić do „ZERA".



Jakie są główne ryzyka związane z bezpieczeństwem IT?

MOŻLIWE WEKTORY ATAKÓW

1. Poczta elektroniczna (poczta służbowa, poczta prywatna)
2. Strony internetowe (spreparowane strony www, strony ze złośliwym kodem)
3. Infrastruktura teleinformatyczna (serwery, sieć LAN/WAN)
4. Fizyczne (podsłuchy, monitoring, dokumenty)

Ryzyko ataków na organizację?

Mitygacja ryzyka powinna obejmować wszystkie wyżej wymienone obszary!

PRZYKŁAD ATAKÓW – POCZTA ELEKTRONICZNA

Przejęcie kontroli nad komputerem – fałszywy email

Wyślij

Do... bok@xxx.pl

DW...

Temat INFORMACJA O ZAMIARZE WSZCZĘCIA KONTROLI SKARBOWEJ

Urząd Skarbowy doręczył zawiadomienie o zamiarze wszczęcia kontroli w dniu 18.04.2016r. Wobec braku możliwości nawiązania kontaktu telefoniczn
jego siedzibie w dniu 6.04.2016r. w celu ustalenia terminu wszczęcia kontroli. Urząd Skarbowy wyznacza termin wszczęcia kontroli na 29.04.2016r. o

Jednocześnie Urząd Skarbowy informuje, że zgodnie z art. 92a ustawy z dnia 13 października 1998r. (Dz. U. z 2007 r., Nr 11, poz.74 z późn. zm.) w z
swobodzie działalności gospodarczej (Dz. U. z 2007 r., Nr 155, poz. 1095 z późn. zm.) czynności kontrolnych dokonuje się w obecności kontrolowane
wyżej wymienionym terminie jest Pani/Pan zobowiązana/y do obecności w siedzibie swojej Firmy i współpracy z inspektorem kontroli. Ponadto zgodni
gospodarczej jest Pani/Pan zobowiązany do pisemnego wskazania osoby upoważnionej do reprezentowania Pani/Pana w trakcie kontroli, w szczególn

Jest Pani/Pan zobowiązana/y do przygotowania wszystkich potrzebnych dokumentów związanych z prowadzoną przez Panią/Pana Firmą wymienionyc

Załącznik do pobrania

Nieobecność Pani/Pana może zostać uznana za stan wyczerpujący znamiona wykroczenia określonego w art. 98 ust. 1 pkt 3 ustawy z 13 października

———————————

INSPEKTOR KONTROLI
Urząd Skarbowy
mgr Tomasz Bartkowski

PRZYKŁAD ATAKÓW – SOCJOTECHNIKA

3.7 MLN straty - Podlaski Zarząd Dróg Wojewódzkich

PRZYKŁAD ATAKÓW – PENDRIVE?

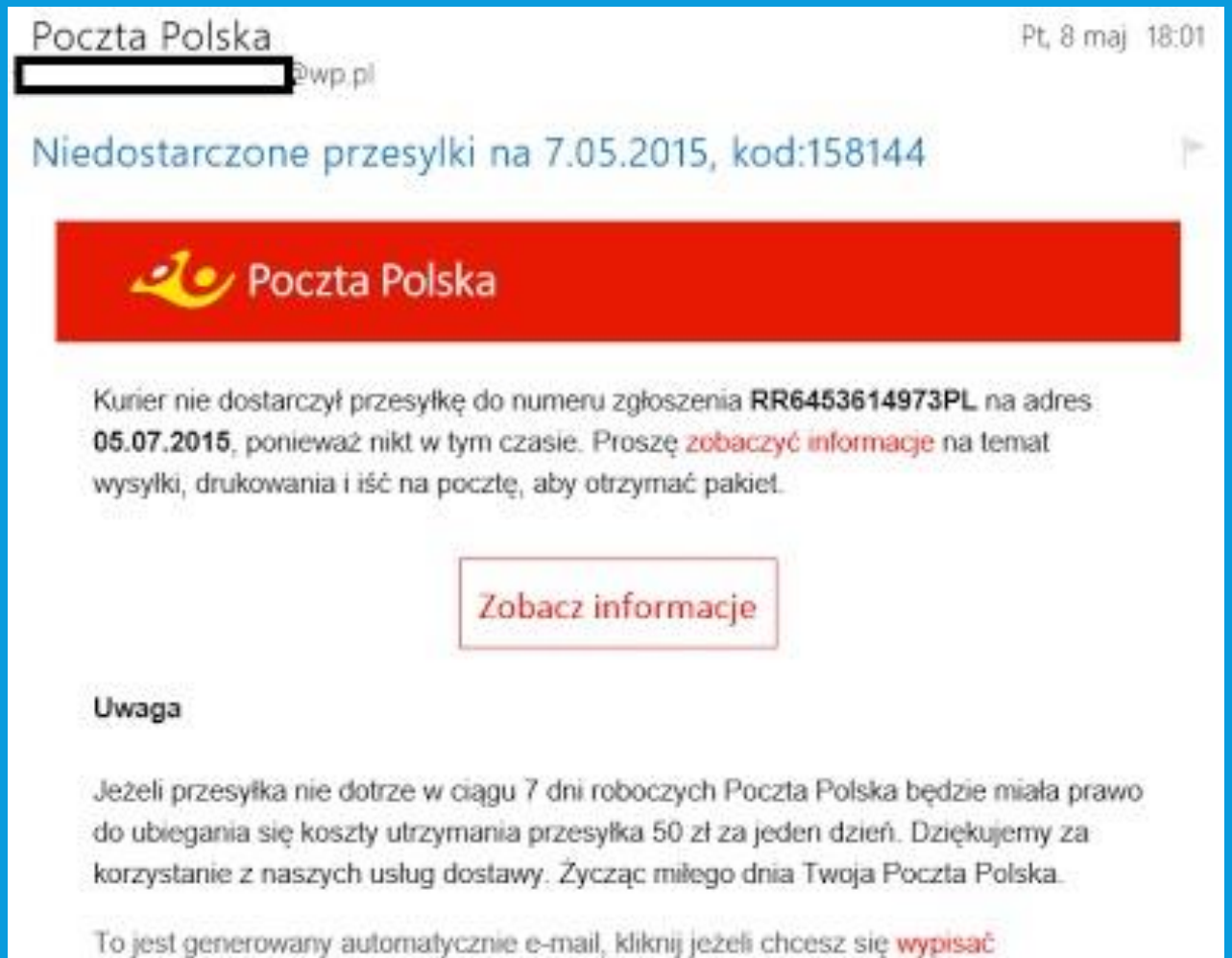
Pendrive reklamowy pozostawiony w biurze

PRZYKŁAD ATAKÓW – DOKUMENTY?

Akta Prokuratury Rejonowej znalezione w sortowni odpadów

PRZYKŁAD ATAKÓW – SPREPAROWANA STRONA WWW

Zaszyfrowanie dysków w urzędzie



Poczta Polska [redacted]@wp.pl Pt, 8 maj 18:01

Niedostarczone przesylki na 7.05.2015, kod:158144

Poczta Polska

Kurier nie dostarczył przesyłkę do numeru zgłoszenia **RR6453614973PL** na adres **05.07.2015**, ponieważ nikt w tym czasie. Proszę zobaczyć informacje na temat wysyłki, drukowania i iść na pocztę, aby otrzymać pakiet.

Zobacz informacje

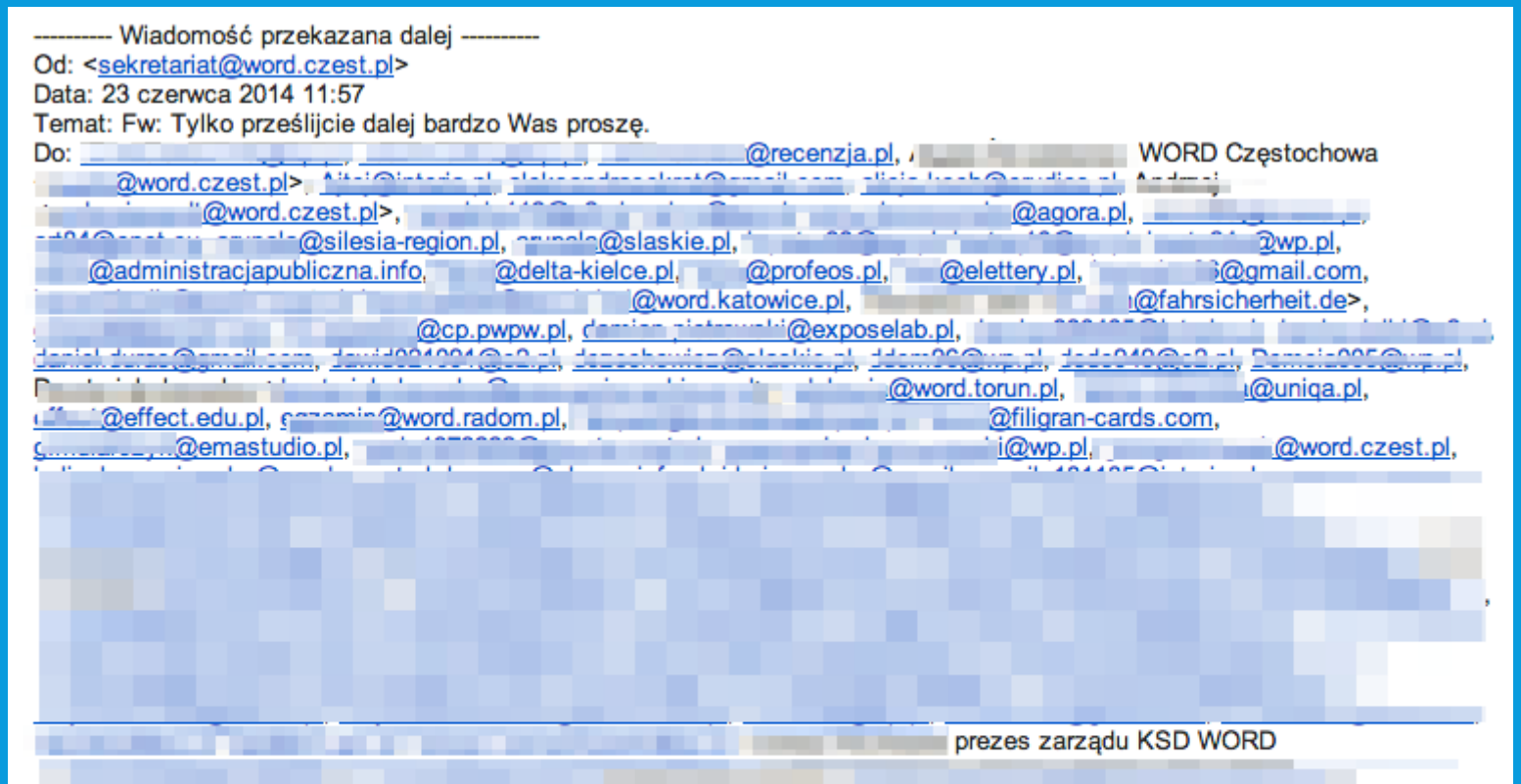
Uwaga

Jeżeli przesyłka nie dotrze w ciągu 7 dni roboczych Poczta Polska będzie miała prawo do ubiegania się koszty utrzymania przesyłka 50 zł za jeden dzień. Dziękujemy za korzystanie z naszych usług dostawy. Życząc miłego dnia Twoja Poczta Polska.

To jest generowany automatycznie e-mail, kliknij jeżeli chcesz się wypisać

PRZYKŁAD BŁĘDU – WYSYŁKA EMAILA

Jedna z pracownic pewnego warszawskiego urzędu przesłała wiadomość do grupy obywateli, ale zamiast w BCC, ich adresy wrzuciła w CC



---------- Wiadomość przekazana dalej ----------
Od: <sekretariat@word.czest.pl>
Data: 23 czerwca 2014 11:57
Temat: Fw: Tylko prześlijcie dalej bardzo Was proszę.
Do: @recenzja.pl, WORD Częstochowa
@word.czest.pl>
@word.czest.pl>,
@agora.pl,
@silesia-region.pl, @slaskie.pl,
@wp.pl,
@administracjapubliczna.info, @delta-kielce.pl, @profeos.pl, @elettery.pl, @gmail.com,
@word.katowice.pl, @fahrsicherheit.de>,
@cp.pwpw.pl, @exposelab.pl,
@word.torun.pl, @uniqa.pl,
@effect.edu.pl, @word.radom.pl, @filigran-cards.com,
@emastudio.pl, @wp.pl, @word.czest.pl,

prezes zarządu KSD WORD

SKUTKI ATAKÓW

1. Wyłudzenie danych osobowych
2. Kradzież danych (informacje przetargowe, dokumenty tajne)
3. Utrata wizerunku (urzędu, instytucji państwowych)
4. Utrata dostępu do e-usług
5. Straty finansowe

JAK MITYGOWAĆ RYZYKO ATAKU?

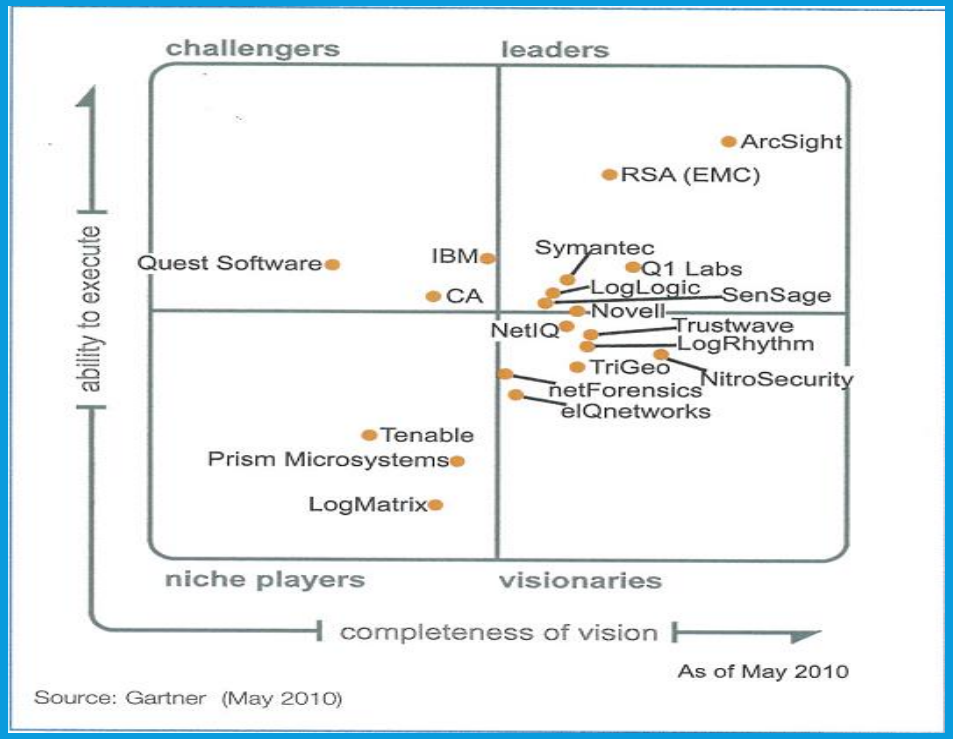
1. Plan zapewnienia bezpieczeństwa
2. Audyty bezpieczeństwa
3. Edukacja pracowników
4. Inwestycje w infrastrukturę IT

JAK MĄDRZE MITYGOWAĆ RYZYKO ATAKU?

1. Kompleksowy plan zapewnienia bezpieczeństwa w różnych obszarach
2. Audyty bezpieczeństwa, certyfikowane, przekrojowe, realizowane przez jednostki zewnętrzne
3. Edukacja, szkolenia, budowanie świadomości bezpieczeństwa jako proces
4. Efektywne inwestycje w infrastrukturę IT, dywersyfikacja technologii

PRZYKŁAD - SIEM, CZYLI JAK WYBIERAĆ ROZWIĄZANIE INFORMATYCZNE

- Co chronimy?; Jaki jest cel? (jakie są wymagania biznesowe i formalno-prawne)
- Wymagania funkcjonalne, jakie stawiamy przed rozwiązaniem? = Zapisy w SIWZ
- Jak wybrać rozwiązanie lub zawęzić poszukiwania?



CYKL PDCA I PO CO MI TO?
(DOBRA PRAKTYKA W BEZPIECZEŃSTWIE)

- **PDCA** (cykl Deminga) to schemat ilustrujący podstawową zasadę ciągłego ulepszania (ciągłego doskonalenia, Kaizen), stworzoną przez Williama Edwardsa Deminga, amerykańskiego specjalistę statystyka pracującego w Japonii.

- **ZAPLANUJ** (ang. Plan): Planuj każdą zmianę z wyprzedzeniem. Przeanalizuj obecną sytuację oraz potencjalne skutki zmian zanim jakiekolwiek podejmiesz. Z góry przemyśl, co powinieneś zmierzyć, aby przekonać się, czy zrealizowałeś swój zamiar. Zaplanuj pomiar, jako jeden z elementów realizacji zmiany. Myśl o pomiarze aż do następnego kroku (przez cały okres planowania). Opracuj plan wdrożenia zmiany, zadbaj przy tym o pełną obsadę tego przedsięwzięcia właściwym personelem oraz zaangażuj właścicieli procesów.

- **WYKONAJ, ZRÓB** (ang. Do): Przeprowadź pilotażowe wdrożenie zmiany w małej skali, w kontrolowanych warunkach (tzn. najpierw przeprowadź eksperyment, bądź zbuduj prototyp).

- **ZBADAJ** (ang. Study): Gruntownie przeanalizuj rezultaty eksperymentu. Wyprowadź wnioski - co zebrane dane mówią na temat skuteczności próbnego wdrożenia?

- **ZASTOSUJ, DZIAŁAJ** (ang. Act): Podejmij właściwe działania, aby wdrożyć standard takiego procesu, który wytworzył rezultaty najbardziej pożądane.

CO WARTO PRZECZYTAĆ?

- **Założenia Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej,** Ministerstwo Cyfryzacji
- **ABC zagrożeń bezpieczeństwa danych osobowych w systemach teleinformatycznych** (GIODO)
- **Raporty** NASK, CERT, ORANGE LABS
- **Raport Zapewnienie bezpieczeństwa działania systemów informatycznych wykorzystywanych do realizacji zadań publicznych,** NIK
- **Stan cyberbezpieczeństwa polskich urzędów,** D. Lisiak, M. Szmit
- **Standardy i dobre praktyki producentów rozwiązań**

PODSUMOWANIE

Bezpieczeństwo to proces

który zmienia się w raz z organizacją i jej potrzebami.
Nie wolno spocząć na laurach.

- Monitorowanie i samodoskonalenie jest priorytetem.