Big Brother

czy bezpieczeństwo IT?

EDUKACJA

BUDOWANIE ŚWIADOMOŚCI

Jaki związek ma podglądanie z bezpieczeństwem?

osób odpowiedzialnych za IT w polskich firmach uważa, że wdrożenie narzędzi do monitorowania podniosłoby poziom bezpieczeństwa ich sieci.

Raport „Bezpieczeństwo. Ryzyko. Dostępność.", TNS na zlecenie HP Polska

Agenda

Po co monitorować?

Jak to zrobić?

Czego unikać?

KORZYŚCI

Wzrost wydajności

90 minut

Od momentu poinformowania pracowników o stosowaniu oprogramowania monitorującego ich aktywność, poświęcają oni dziennie na pracę średnio 90 minut więcej.

Boston Globe: Firms step monitoring employee activities

Efektywne zarządzanie licencjami

181 mln

Właściwe zarządzanie licencjami na oprogramowanie może przynieść olbrzymie oszczędności. Jedna z głównych agencji federalnych z USA zaraportowała, że tylko w 2012 roku udało się jej zaoszczędzić z tego tytułu aż 181 mln USD.

Government Accountability Office USA

Bezpieczeństwo

wycieków danych spowodowanych jest nieuprawnionym i często nieświadomym działaniem pracowników.

Raport B2B International i Kaspersky Lab

Zaledwie 5% wszystkich przypadków utraty danych było spowodowanych przez ataki z zewnątrz.

Raport HP Polska dla biznesu

KONSEKWENCJE

Atak na polskie samorządy

Phishing podszywający się pod aktualizację oprogramowania BeSTi@ do zarządzania budżetami jednostek samorządu terytorialnego.

niebezpiecznik.pl

From: Pomoc BeSTi@ [mailto...@budzetjsf.pl]
Sent: Monday, March 17, 2014 8:49 AM
To:...
Subject: Aktualizacja systemu BeSTi@ do wersji 3.02.012.07

Witamy,
Pragniemy poinformować, iż dnia dzisiejszego została udostępniona nowa aktualizacja do systemu BeSTi@ w wersji 3.02.012.07.
Aktualizacja usuwa błędy związane z bezpieczeństwem bazy danych oraz poprawia problem z podpisem elektronicznym sprawozdań.

Instalacja jest bardzo prosta i nie wymaga dodatkowej pomocy oraz czynności.
Ze względu na znaczące poprawki bezpieczeństwa aktualizacja nie jest dostępna z menu programu BeSTia, należy przeprowadzić ją ręcznie.

Poniższy plik "Bestia.3.02.012.07" należy zapisać na pulpicie lub w innym miejscu a następnie go uruchomić co spowoduje zainstalowanie uaktualnienia do systemu BeSTi@.

hxxp://budzetjsf.pl/Update/BeSTia/Bestia.3.02.012.07.exe

Instalacja nie powinna zająć więcej niż minutę.
Dziękujemy i przepraszamy za niedogodności

———————

Sputnik Software
tel. 61 622 00 60

Niekontrolowany wypływ pieniędzy

Malware podmieniający numer konta na konto cyberprzestępców podczas kopiowania ze schowka Windows.

Cert.pl

Niekontrolowany wypływ pieniędzy

Pracownik Podlaskiego Zarządu Dróg Wojewódzkich przelał 3,7 miliona złotych na podstawione konto bankowe.

Rzeczpospolita

Niekontrolowany wypływ pieniędzy

500 000 złotych wyciekło z konta Gminy Rząśnia po ataku hakerskim.

gazeta.pl

ODPOWIEDZIALNOŚĆ

Odpowiedzialność prawna

- odpowiedzialność pracownicza (dyscyplinarna) – art. 100 § 2 pkt. 4, art. 114 i art. 120 Kodeksu Pracy
- odpowiedzialność cywilna (odszkodowawcza) – art. 23-24 i 415 Kodeksu Cywilnego

Odpowiedzialność prawna

- szczególna sankcja karna – art. 36, art. 39a i art. 52 Ustawy o Ochronie Danych Osobowych
- baza danych – art. 11-12a Ustawy o Ochronie Baz Danych
- odpowiedzialność branżowa, np. dane wrażliwe, tajemnica zawodowa itp.

NIEBEZPIECZNA GRA

Korzystanie z Internetu

1godz. 11 min

Tyle średnio dziennie spędzają pracownicy na portalach niezwiązanych ze swoimi obowiązkami. Są wtedy bardziej narażeni na atak cyberprzestępców.

Raport TimeCamp

Nielegalne treści i oprogramowanie

To odsetek nielicencjonowanych kopii oprogramowania zainstalowanego na firmowych komputerach w 2016 roku.

Business Software Alliance (BSA)

1mln USD

musiała zapłacić firma ze wschodniej Polski, w sieci której znaleziono ponad 200 nielegalnych programów.

Business Software Alliance (BSA)

Nieautoryzowany dostęp fizyczny

Polaków deklaruje, że bardzo często wykorzystuje prywatny sprzęt mobilny w pracy. Co piąty jest gotów złamać firmową politykę bezpieczeństwa, by to robić.

Raport Fortinet

firm nie ma pewności, gdzie zlokalizowane są ich poufne dane, a ponad połowa martwi się, że mogą zostać wyniesione przez pracowników tymczasowych.

Raport Data Security Intelligence / Ponemon Institute

Malware preinstalowany w kamerach CCTV

Zainfekowane kamery można było zakupić w sklepie Amazon.

thehackernews.com

E-papierosy z wirusami

Komputery były infekowane podczas ładowania urządzenia przez port USB.

The Guardian

Anonimizacja

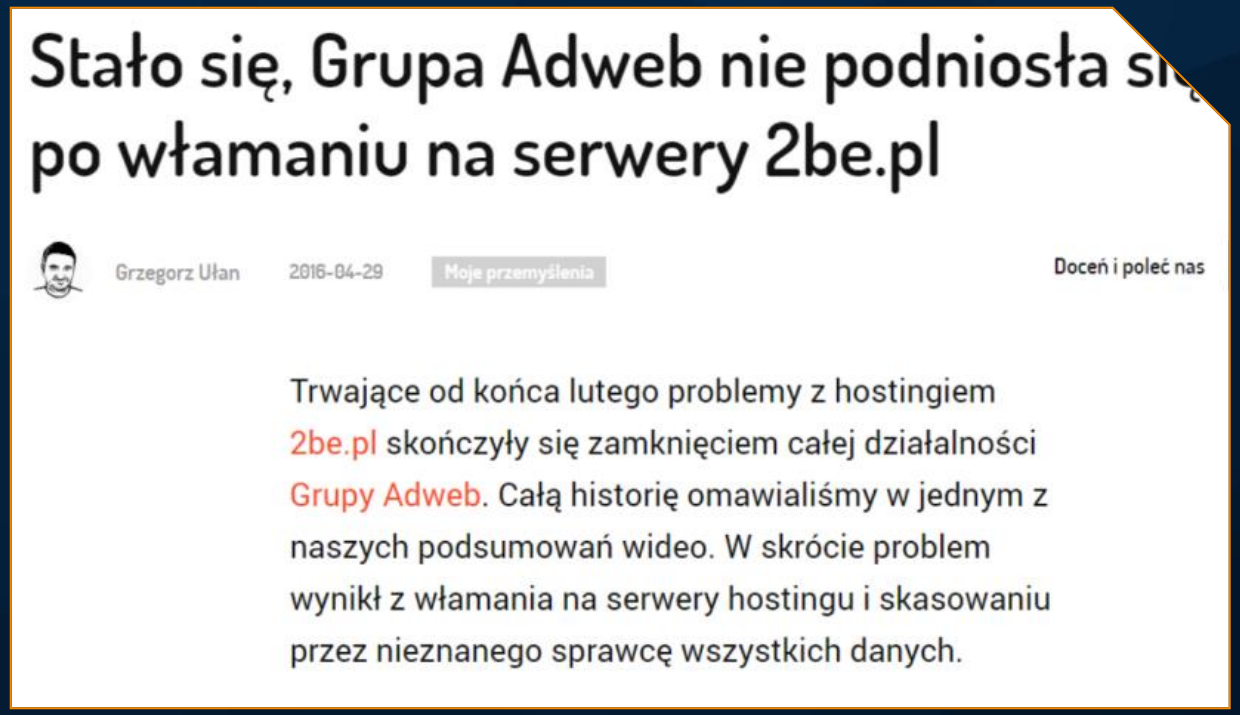
Istnieje wiele narzędzi pozwalających anonimizować ruch w sieci. Co sprytniejsi pracownicy próbują w ten sposób unikać odpowiedzialności, łamią też często prawa autorskie.

KOLEJNE PRZYKŁADY

Utrata lub kradzież danych

Znany przykład grupy Adweb, która powierzyła dostęp do kluczowych usług i serwisów jednemu człowiekowi.

antyweb.pl



Utrata lub kradzież danych

firm, które straciły swoje dane, zostało zamkniętych w ciągu sześciu miesięcy od wycieku.

Badanie The Diffusion Group

firm, które doznały znaczącej utraty danych, zniknęło z rynku w ciągu kolejnych dwóch lat.

Badanie The Diffusion Group

Szokujący fakt

Firm, które utraciły dane na więcej niż 10 dni, bankrutowało w ciągu jednego roku.

Raport British Chambers of Commerce

Straty finansowe

300 tys./h

Badania IDC wykazały, że łączny roczny czas przerw spowodowanych awariami sieci wynosi od 16 do 20 roboczogodzin, co oznacza stratę ~70 000 USD. Największe firmy wg szacunków Gartnera mogą tracić nawet 300 000 USD na godzinę.

IDC / Gartner

Cenna receptura

1 427 900,85 zł

W postępowaniu dowodowym wykorzystano m.in. historię pracy na pliku z recepturą (daty zapisu).

tajemnica-przedsiebiorstwa.pl

Utrata wiarygodności

Pracownik banku sprzedał dane finansowe klientów niemieckiemu fiskusowi.

wp.pl

Pracownik banku zatrzymany za kradzie danych klientów

Szwajcarski bank Julius Baer poinformował, że jego pracownik został zatrzymany w związku z podejrzeniami, iż dopuścił się kradzieży poufnych danych klientów banku. Dane te trafiły później do niemieckich władz podatkowych.

Utrata wiarygodności

Nikt nie może czuć się bezpiecznie.

Polska Agencja Prasowa

Dane nowej szefowej Secret Service w internecie

pap 05.04.2013 06:53

Secret Service, agencja zajmująca się m.in. ochroną prezydenta USA, poinformowała, że bada sprawę kradzieży danych elektronicznych jej nowej szefowej Julii Pierson.

Odpowiedzialność kierownictwa

Za wycieki danych odpowiedzialność w większości ponoszą osoby zarządzające, niekoniecznie pionem IT.

wyborcza.biz

Największa kara...

Top executives resign over massive data leak

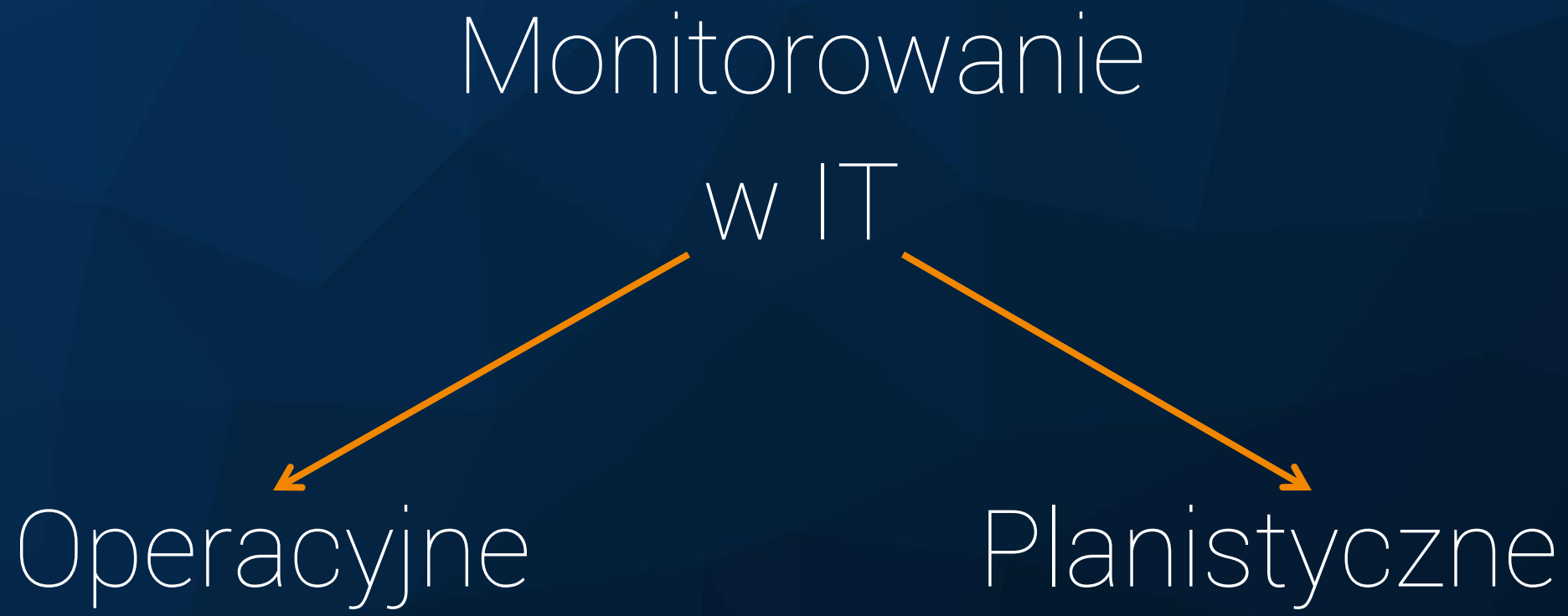
Suspected scams using information stolen from card firms reported

Published : 2014-01-20 2
Updated : 2014-01-20 2

JAK WDROŻYĆ MONITORING?

Cel monitorowania?

Cel monitorowania



Monitorowanie operacyjne

- zarządzanie awariami
- zarządzanie konfiguracją
- zarządzanie bezpieczeństwem

Monitorowanie planistyczne

- zarządzanie wydajnością
- zarządzanie rozliczaniem
- zarządzanie zmianami

Wyzwania prawne

- możliwość „naginania” przepisów przez pracowników i pracodawcę
- trudność z określeniem legalności sposobu monitorowania
- brak wskazania dopuszczalnych sposobów technicznych w obowiązujących przepisach

Uprawnienia pracodawcy

- aktywność w Internecie, kategoryzowanie treści
- dostęp do zasobów
- wykorzystanie aplikacji, instalacja / deinstalacja
- zmiany sprzętowe
- podgląd pulpitu
- aktywność stacji roboczej

Podstawy prawne

- Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.: art. 47, 49 i 51
- Ustawa z dnia 26 czerwca 1974 r. Kodeks Pracy: art. 11, 15, 22 i 94
- Ustawa z dnia 29 sierpnia 1997 r. o Ochronie Danych Osobowych: Rozdział 5
- Ustawa z dnia 6 czerwca 1997 r. Kodeks Karny: art. 218 i 267
- Ustawa z dnia 23 kwietnia 1964 r. Kodeks Cywilny: art. 23 i 24

Najnowsze orzecznictwo

Wyrok Europejskiego Trybunału Praw Człowieka w Strasburgu w sprawie Bogdana Barbulescu.

Należy bezwzględnie poinformować pracowników o tym, że **są monitorowani i w jakim zakresie**. Najlepiej w Regulaminie Pracy lub Umowie.

Rozporządzanie Ministra Pracy i Polityki Socjalnej

Załącznik, pkt. 10, lit. e

Przy projektowaniu, doborze i modernizacji oprogramowania, a także przy planowaniu wykonywania zadań z użyciem ekranu monitora, pracodawca powinien uwzględniać w szczególności następujące wymagania:

(...)

e) bez wiedzy pracownika nie można dokonywać kontroli jakościowej i ilościowej jego pracy.

Czego nam jeszcze nie wolno?

- keylogging
- przeglądanie korespondencji prywatnej
- zrzuty ekranu bez wyraźnych podejrzeń

Proponowana procedura

- plan wdrażania monitorowania i kontroli działań pracowników
- określenie celu monitorowania
- określenie zasad korzystania z infrastruktury IT
- minimalizacja możliwości naruszenia prywatności
- publikacja zasad i przeszkolenie pracowników

Karta użytkownika sprzętu komputerowego

„Ja, niżej podpisana(y), zgadzam się podporządkować i przestrzegać zapisów zamieszczonych w Księdze Bezpieczeństwa Informacji (KBI) oraz oświadczam, że jestem świadom odpowiedzialności oraz wszelkich konsekwencji wynikających z nieprzestrzegania powyższych zasad. Jednocześnie przyjmuję do wiadomości, że Referat Informatyki monitoruje wszelkie czynności wykonywane na komputerze, ruch internetowy oraz wydruki i ma możliwość pracy na komputerze użytkownika."

Polityka bezpieczeństwa

„System komputerowy na każdym stanowisku pracy monitorowany jest pod kątem wszelkich zmian w oprogramowaniu (umożliwiony jest audyt legalności oprogramowania, tworzy się automatycznie historia w zakresie sprzętu i oprogramowania) oraz pełny monitoring wykorzystywania aplikacji roboczej (użytkowanie aplikacji i historia pracy).”

EDUKACJA

BUDOWANIE ŚWIADOMOŚCI

Czego unikać?

- łamania prawa
- trzymania pracowników w niewiedzy
- przesadnej kontroli i utraty zaufania
- traktowania ludzi jak maszyny
- zrzucania odpowiedzialności za bezpieczeństwo IT
- naruszania prywatności pracowników

DZIĘKUJĘ ZA UWAGĘ

axence.net