Zakończenie wsparcia dla Windows XP a bezpieczeństwo systemów teleinformatycznych

Daniel Grabski e-mail: danielgr@microsoft.com
Chief Security Advisor
Microsoft

Świat informatyki w roku 2001

Computers & mobile

Internet i social

z

~361 mln

użytkowników Internetu w 2000 r.

do

~2,4 mld w 2012 r.

Brak Facebook'a, Twitter'a, YouTube'a

Cloud

Big data

Technologia dzisiaj i jutro

Mobile

Do **2016 r. smartphony** i **tablety** znajdą się w posiadaniu ponad miliarda konsumentów

Liczba pracowników **mobilnych** osiągnie poziom **1.3 mld** do **2015 r.** co stanowi ponad **37%** wszystkich pracujących.

Social

Millennials (cyfrowe pokolenia) będzie stanowiło **75%** wszystkich amerykańskich pracowników do **2025 r.**

65% firm deklaruje, że wdraży przynajmniej jedno narzędzie typu **social software**.

Cloud

Ponad **80%** nowych aplikacji **będzie dystrybuowana lub wdrażana w cloudzie w 2012 r.**.

70% organizacji używa lub rozważa użycie rozwiązań opartych na przetwarzaniu w chmurze

Big data

Kontent cyfrowy wzrośnie do 2.7ZB w 2012, wzrost o 48% od 2011 r., dynamika wzrostu prognozuje poziom **8ZB do 2015 r**.

80% **wzrost** nieustrukutyzowanych danych w ciągu n **następnych 5 lat**.

Cyber Security

Gwałtownie rosnąca ilość **tożsamości** oraz urządzeń powoduje wyzwania związane z tożsamością oraz zarządzaniem dostępem

250% wzrost złośliwego oprogramowania „dedykowanych" na urządzenia mobilne (mobile malware)

300k social identities compromised every day

Security, **Access** i **Privacy** coraz bardziej istotne

Jeśli, nie **bardziej ważne niż** **cechy**, **funkcje** i cena

Ataki i ich sprawcy używają coraz bardziej zaawansowanych technik. Tradycyjne metody obrony są niewystarczające

Spy Thief Vandal Hacker Author

Jakie są ryzyka związane z pozostaniem na XP?

Atakujący będą mieli przewagę nad broniącymi się

Po zakończeniu wsparcia dla XP, w momencie kiedy będą ogłaszane biuletyny bezpieczeństwa dla supportowanych wersji systemu operacyjnego, atakujący poprzez tzw. reverse engineer będą w stanie zidentyfikować czy występują w one XP

Jeśli Windows XP będzie posiadał w/w podatności atakujący zbuduja tzw. exploit code aby włamać się do systemu

W związku z faktem, że update'y bezpieczeństwa dla Windows XP nie będą już nigdy dostępne aby odpowiedzieć na nowe podatności, po 8 kwiewtnia 2014 system ten będzie posiadał tzw. podatność "0 day" na zawsze !!!

Pomiędzy lipcem 2012 a lipcem 2013 Windows XP występował w 45 biuletynach bezpieczeństwa, z których 30 dotyczyło również Windows 7 i Windows 8

Zagrożenia w obszarze cyberbezpieczeństwa

1995

Kluczowe zagrożenia
- Rozwój Internetu
- Początek usług pocztowych

Windows 95

2001

Kluczowe zagrożenia
- Wirus Melissa (1999), List miłosny - Love Letter (2000)
- Wykorzystanie inżynierii społecznej

Windows XP
- Login (Ctrl+Alt+Del)
- Kontrola Dostępu
- Profile użytkownika
- Polityki/profile bezpieczeństwa
- Szyfrowanie plików
- Smartkarty i wsparcie PKI
- Windows Update

2004

Kluczowe zagrożenia
- Code Red and Nimda (2001), Blaster (2003), Slammer (2003)
- Przepełnienie bufora
- Script kiddies (haker niższej rangi)
- Czas od uaktualnienia do napisania złośliwego oprogramowania liczony w tygodniach

Windows XP SP2
- Address Space Layout Randomization (ASLR)
- Data Execution Prevention (DEP)
- Wprowadzenie metodyki Security Development Lifecycle (SDL)
- Auto Update domyślnie
- Firewall domyślnie
- Windows Security Center
- Wsparcie WPA

2007

Kluczowe zagrożenia
- Robak Zotob (2005)
- Atak na warstwę aplikacji
- Rootkity
- Przepełnienie bufora
- Script Kiddies
- Wzrost Phishing'u
- Użytkownik na koncie administratora

Windows Vista
- Bitlocker
- Patchguard
- Ulepszony ASLR i DEP
- Pełny SDL
- User Account Control
- Internet Explorer Smart Screen Filter
- Digital Right Management
- Ulepszony Firewall
- Wymóg podpisywania sterowników
- Wsparcie TPM
- Windows Integrity Levels
- Bezpieczna konfiguracja "by default" (Windows i Przeglądarka IE)

2009

Kluczowe zagrożenia
- Zorganizowana przestępczość cyfrowa
- Sieci Botnet
- Kradzież tożsamości
- Robak Conficker (2008)
- Czas od uaktualnienia do napisania złośliwego oprogramowania liczony w dniach

Windows 7
- Ulepszony ASLR i DEP
- Pełny SDL
- Ulepszony IPSec
- Managed Service Accounts
- Ulepszony User Account Control
- Enhanced Auditing
- Internet Explorer Smart Screen Filter
- AppLocker
- BitLocker to Go
- Windows Biometric Service
- Windows Action Center
- Windows Defender

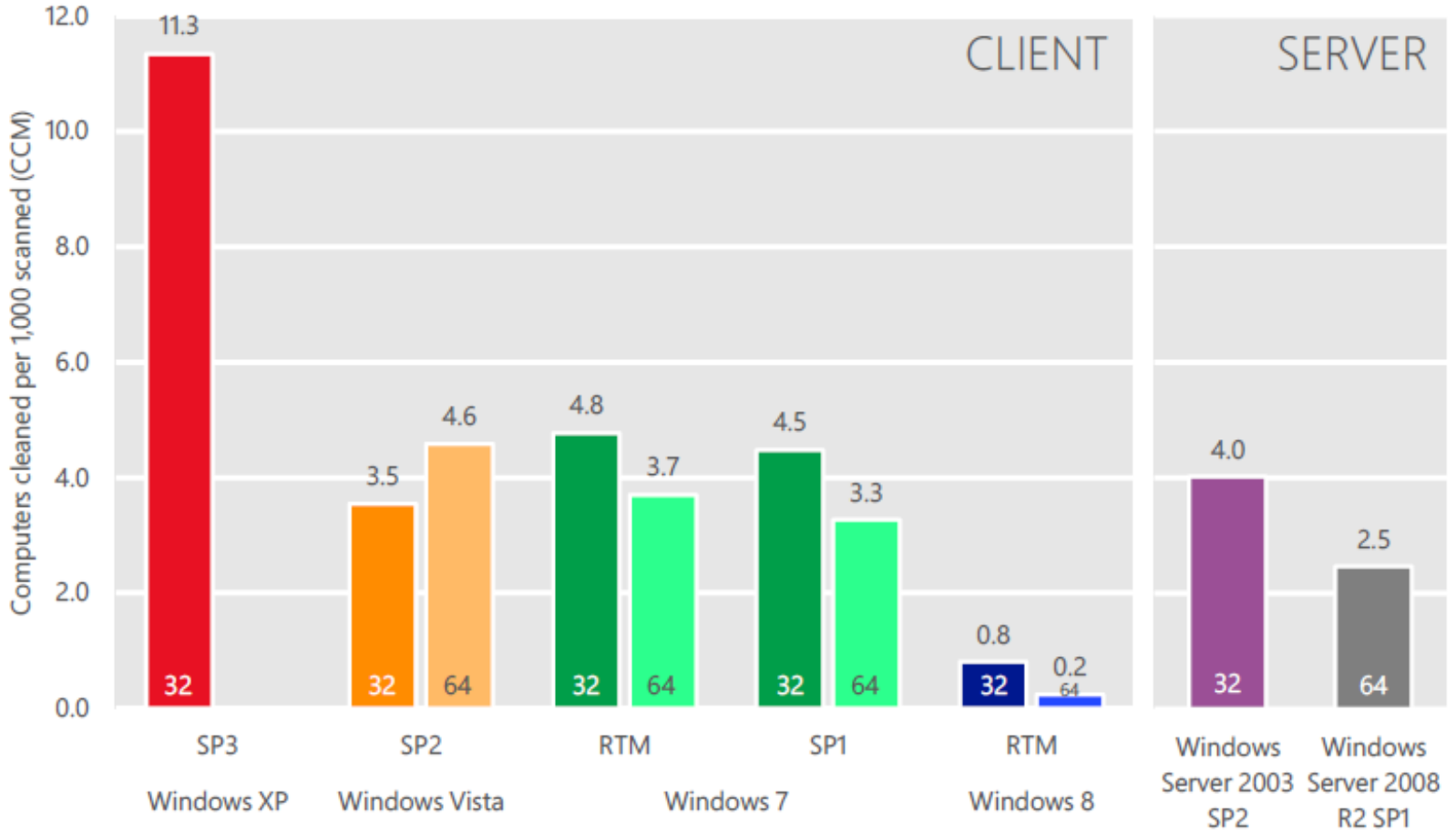
2012

Kluczowe zagrożenia
- Zorganizowana przestępczość cyfrowa, potencjalny udział przedstawicieli instytucji rządowych
- Ataki ukierunkowane (Targeted Attacks)
- Operacja Aurora (2009)
- Wirus Stuxnet (2010)
- Wirus Flame (2012)

Windows 8
- UEFI (Secure Boot)
- Firmware Based TPM
- Trusted Boot (z ELAM)
- Measured Boot i Remote Attestation Support
- Znaczące zmiany w ASLR i DEP
- AppContainer
- Windows Store
- Internet Explorer 10 (Plugin-less and Enhanced Protected Modes)
- BitLocker: Encrypted Hard Drive and Used Disk Space Only Encryption Support
- Virtual Smartcard
- Hasło obrazkowe, PIN
- Dynamic Access Control
- Wbudowany Antywirus

Efekt wdrożonych przedsiewzięć w obszarze bezpieczeństwa

Nowszy = bardziej bezpieczny



"32" = 32-bit edition; "64" = 64-bit edition. SP = Service Pack. RTM = release to manufacturing. Operating systems with at least 0.1 percent of total MSRT executions in 4Q12 shown.

Weźmy pod uwagę, że:

- Cyberprzestępcy wiedzą o końcu wsparcia dla Windows XP oraz że po 8 kwietnia 2014 r. żadne update'y do tego systemu nie będą dostępne

- Nie migrując do najnowszej platformy narażamy się na bycie łatwym celem dla cyberprzestępców

- XP był wspaniałym systemem operacyjnym (na swoje czasy)

- Zwiekszony poziom zainfekowania Windows XP możemy przypisać faktycznie temu, że kluczowe funkcjonalności i rozwiązania w obszarze security zaimplementowane w ostatnich wersjach systemu Windows nie są obecne w systemie Windows XP. System Windows XP został zaprojektowany w innych czasach, w innej erze i po prostu nie jest w stanie łagodzić i zapobiegać zagrożeniom tak efektywnie jak nowsze wersje systemu operacyjnego Windows 7 i Windows 8.

Co mówią analitycy

“Wielu producentów oprogramowania (ISVs) przestaje wspierać nowe wersje oprogramowania na Windows XP w 2011, pozostali w roku 2012.”

- Michael Silver (June 2011)

“Istniejące luki bezpieczeństwa nie zostaną całkowicie wyeliminowane a nowe są bardzo prawdopodobne do odnalezienia. Luki które Microsoft naprawia w Windowsach (np. Windows Vista, Windows 7 and Windows 8) które nadal będą wspierane po zakończeniu wsparcia XP mogą być łatwiejsze do zidentyfikowania przez hakerów, jeśli występują.”

- Michael Silver, Stephen Kleynhans (Jan 2013)

“Lepiej jest wydać pieniądze na migrację z Windows XP w 2013 zamiast wydawać je na Custom Support dla Windows XP w latach 2014 & 2015.”

- Michael Silver, Stephen Kleynhans (Jan 2013)

Gartner®

Cyberbezpieczeństwo w administracji publicznej w Polsce

- „Polityka ochrony cyberprzestrzeni RP”.
  - Porządkuje strukture organizacyjną, nakłada nowe role i obowiązki dla administracji publicznej (AP) w tym obszarze:
  - PBC – Pełnomocnik ds. Bezpieczeństwa Cyberprzestrzeni w jednostkach organizacyjnych AP
  - W każdej jednostce administracyjnej administracji rządowej w ramach zapewnienia bezpieczeństwa cyberprzestrzeni, kierownik jednostki powinien ustanowić system zarządzania bezpieczeństwem informacji w oparciu o obowiązujące przepisy i najlepsze praktyki
  - Raportowanie do ministra właściwego ds. Informatyzacji (do 31 stycznia), raport dla Premiera RP (marzec)
  - Współpraca administracji publicznej w obszarze cyberbezpieczeństwa z dostawcami ICT

Rozporządzenie: Krajowe Ramy Interoperacyjności (KRI)

KRI.pdf - Adobe Reader

File Edit View Window Help

7 / 18 117% Tools Sign Comment

At least one signature has problems. Signature Panel

12) zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:

a) dbałości o aktualizację oprogramowania,

b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,

c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,

d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,

e) zapewnieniu bezpieczeństwa plików systemowych,

f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,

g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,

h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;

13) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;

14) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

3. Wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym:

1) PN-ISO/IEC 17799 – w odniesieniu do ustanawiania zabezpieczeń;

2) PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem;

3) PN-ISO/IEC 24762 – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania

Sign In

Export PDF

Adobe ExportPDF

Convert PDF files to Word or Excel online.

Select PDF File:

KRI.pdf

1 file / 1.08 MB

Convert To:

Microsoft Word (*.docx)

Recognize Text in English(U.S.)

Change

Convert

Create PDF

Send Files

Store Files

10:25

2013-09-30

Ile Windows XP w administracji publicznej

http://ranking.pl/pl/rankings/operating-systems.ht

Systemy operacyjne » gemi...

KRAJE

WOJEWÓDZTWA

POZIOM AKCEPTACJI COOKIES

RUCH PC VS. NON-PC

SYSTEMY OPERACYJNE

XLS

Lp.	Nazwa	16.09-22.09.2013	09.09-15.09.2013	02.09-08.09.2013
1	Windows 7	47.07%	46.95%	47.10%
2	Windows XP	29.22%	29.49%	29.58%
3	Windows Vista	7.78%	7.83%	7.85%
4	Windows 8	6.09%	5.90%	5.75%
5	Android	5.08%	5.06%	4.97%
6	iOS	1.77%	1.78%	1.76%
7	Linux	0.98%	0.98%	1.00%
8	Mac OS X	0.93%	0.94%	0.94%
9	Symbian	0.28%	0.28%	0.28%
10	Windows Phone 7	0.25%	0.25%	0.26%
Wielkość próby (liczba odsłon)		3 884 294 296	3 826 501 297	3 698 102 247

Pokaż wartości bezwzględne

Znajdź:

Informujemy, że zmiany, które są widoczne w wynikach rankingu systemów operacyjnych dla Mac OS X i iOS są wynikiem planowanej aktualizacji procesu rozpoznawania systemów operacyjnych, która miała miejsce wraz z publikacją danych za tydzień 24.10.2011-30.10.2011. W przypadku jakichkolwiek pytań związanych z w/w zmianą prosimy o kontakt.

12:16
2013-09-29

Rekomendacja CERT GOV

http://www.cert.gov.pl/portal/cer/9/587/Microsoft

Microsoft - Koniec wsparci...

wpisz szukaną frazę

CERT.GOV.PL

STRONA GŁÓWNA | O NAS | ZGŁASZANIE INCYDENTU | PRACA W CERT | POLITYKA PRYWATNOŚCI | MAPA SERWISU | WYSZUKIWARKA

- Strona główna
- Wiadomości
  - Poprawki i aktualizacje
  - Zagrożenia i podatności
  - Wiadomości ogólne
- System ARAKIS-GOV
- Szkolenia
- Publikacje
- Narzędzia
- Zalecenia konfiguracyjne
- FAQ
- Linki
- Kontakt
- Klucz PGP

ZGŁASZANIE INCYDENTU

Strona główna › Wiadomości › Wiadomości ogólne

Microsoft - Koniec wsparcia dla Windows XP

W ramach współpracy prowadzonej przez Microsoft i Agencję Bezpieczeństwa Wewnętrznego w programie SCP (Security Cooperation Program), którego jednym z elementów jest podnoszenie świadomości społecznej w zakresie security, informowanie o zagrożeniach w zakresie bezpieczeństwa teleinformatycznego oraz proaktywne przeciwdziałanie im przypominamy, że 8 kwietnia 2014 roku zakończy się wsparcie dla następujących produktów Microsoft:

- Windows XP SP3
- Microsoft Exchange Server 2003
- Office 2003
- Microsoft Office SharePoint Server 2003

Co to oznacza w praktyce ?

Po 8 kwietnia 2014 r. nie będą udostępniane nowe poprawki zabezpieczeń, poprawki niedotyczące zabezpieczeń, bezpłatne lub płatne wsparcie techniczne i aktualizacje zawartości technicznej online. Dla systemów, które z różnych powodów nie będą gotowe do przejścia na nowszą platformę po 8 kwietnia 2014 r. Microsoft przygotowuje płatną usługę wsparcia, której koszty będą wyższe niż standardowa oferta tego typu.

Działanie systemu Windows XP SP3, Microsoft Exchange Server 2003 i pakietu Office 2003 w danym środowisku po upływie daty zakończenia świadczenia

Najbardziej popularne

Wznowienie cyklu szkoleń dla administracji rządowej i samorządowej w 2013r.

15.01.2013

Pomiędzy II a IV kwartałem 2013 planowane jest przeprowadzenie kolejnej serii bezpłatnych szkoleń dla administratorów systemów teleinformatycznych administracji publicznej. Szkolenia oferowane są w ramach współpracy Agencji Bezpieczeństwa Wewnętrznego z firmą Microsoft w zakresie bezpieczeństwa teleinformatycznego SCP (Security Cooperation Program).

więcej

Kradzieże haseł - ostrzeżenie

01.03.2012

W związku z powtarzającymi się incydentami teleinformatycznymi na różnego typu stronach internetowych, w rezultacie których zostają wykradzione hasła użytkowników, zespół CERT.GOV.PL przypomina podstawowe zasady bezpieczeństwa:

więcej

Wyciąg z ogólnej analizy ataków na witryny administracji państwowej RP w okresie 21 - 25 stycznia 2012r.

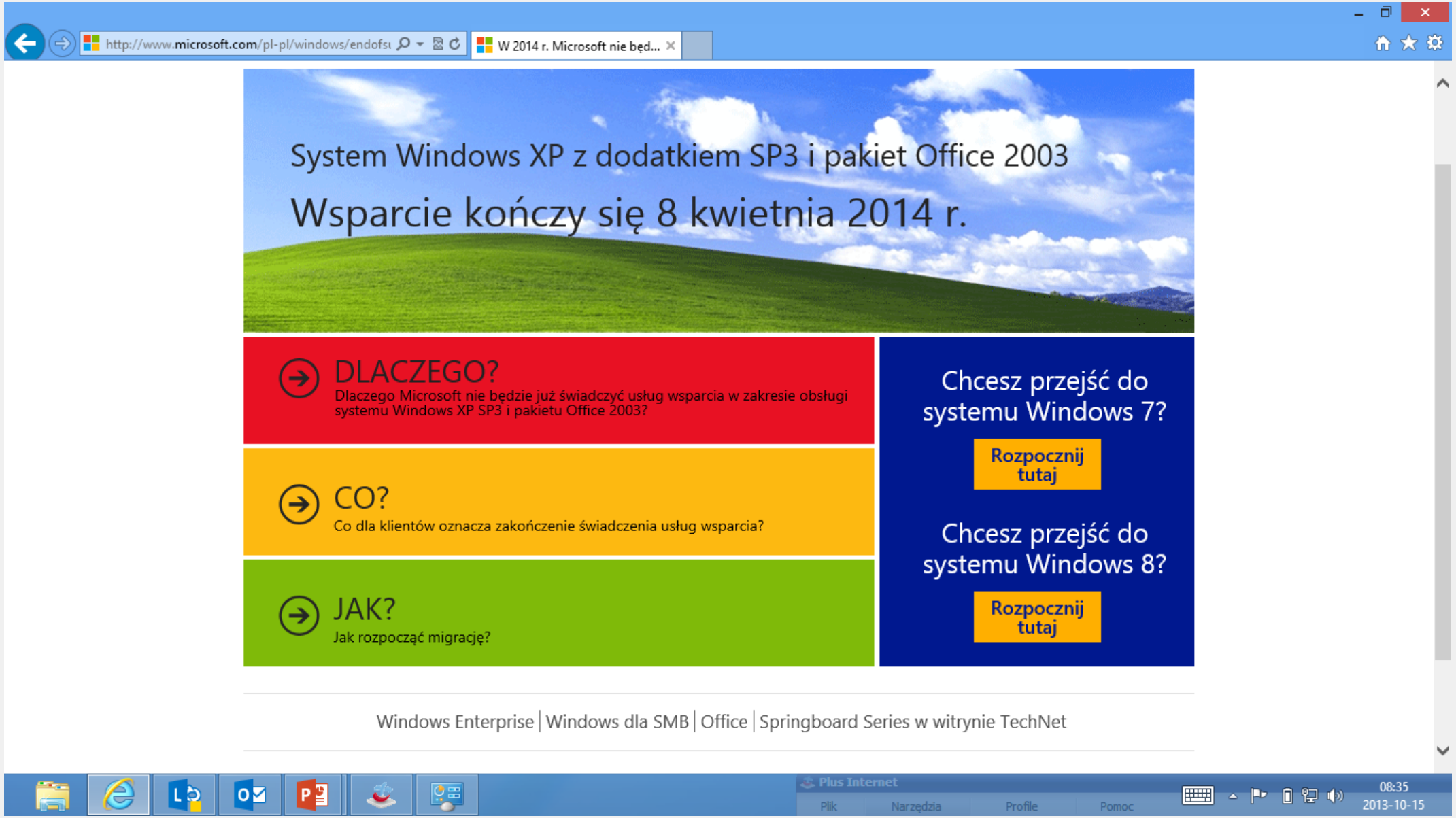
13.02.2012

Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL opracował analizę ataków na witryny

13:34
2013-09-29

Kampania szkoleniowa pod patronatem ABW i CERT GOV

Wiecej informacji http://www.microsoft.com/pl-pl/windows/endofsupport.aspx



Wiecej informacji

http://www.microsoft.com/pl-pl/windows/endofsupport.aspx

Przydatne linki:
http://www.cert.gov.pl/portal/cer/33/Microsoft_Windows.html - praktyczne przewodniki dotyczace ustawień bezpieczeństwa dla systemów Windows 7 i Windows 8

http://www.cert.gov.pl/portal/cer/9/587/Microsoft__Koniec_wsparcia_dla_Windows_XP.html?search=738242659 – rekomendacja dotycząca zakończenia wsparcia dla Windows XP przez CERT GOV PL

www.bip.msw.gov.pl/download/4/953/kri.pdf - Krajowe Ramy Interoperacyjności

http://mac.bip.gov.pl/prawo-i-prace-legislacyjne/polityka-ochrony-cyberprzestrzeni-rp-resortowe-zglaszanie-uwag-do12-10-2012.html - Polityka Ochrony Cyberprzestrzeni RP