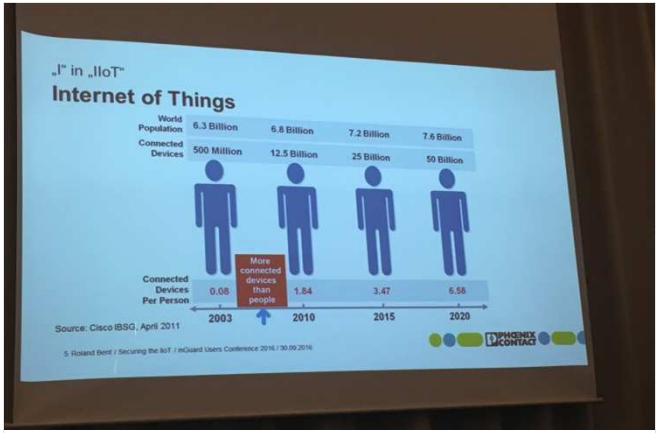
Cyberbezpieczeństwo

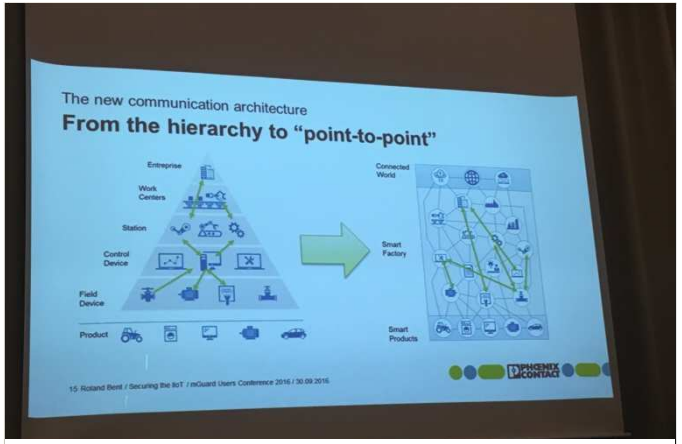
Spojrzenie z perspektywy zarządu organizacji

Cyberbezpieczeństwo

Skąd taki wzrost zagrożenia ?



Lawinowo rośnie liczba urządzeń podłączanych do sieci
Szacuje się, że już około roku 2007 liczba podłączonych urządzeń była większa niż liczba ludzi na świecie



Zmienia się model komunikacji, hierarchię wypiera struktura sieciowa („każdy z każdym")
Rośnie zapotrzebowanie na serwisy on-line, chcemy być w sieci 24/7

Cyberbezpieczeństwo

Prawdy oczywiste

- Jeżeli coś może być podłączone do internetu, **będzie podłączone**
- **Każde** urządzenie podłączone do internetu zapewnia łączność dwukierunkową; może zatem stanowić potencjalne zagrożenie (także licznik energii, termostat itp.)
- Nie ma instytucji, firm, osób, które są w pełni odporne na cyberataki; można jedynie **minimalizować** zagrożenia

Cyberbezpieczeństwo

Mapa zagrożeń

Kto stwarza zagrożenia ?

- Użytkownik komputera (pracownik / były pracownik), świadomie lub nieświadomie
- Hakerzy / społeczności hakerskie
- Zorganizowana cybeprzestępczość
- Agendy rządowe

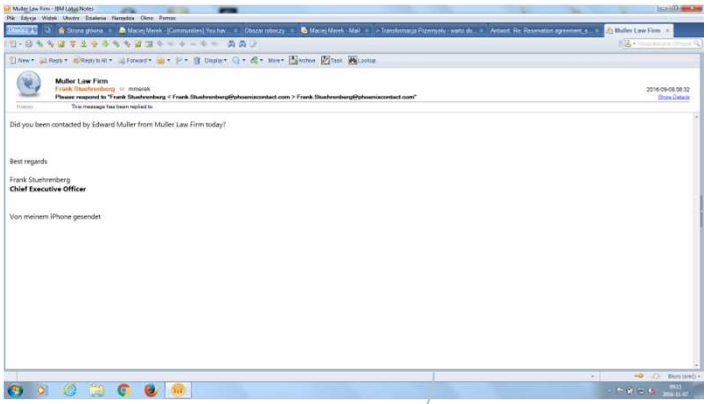
Skutek działania

- Denerwowanie, zakłócanie pracy, wywołanie irytacji
- Kradzież danych personalnych (klientów, pracowników)
- Niszczenie danych / infrastruktury na poziomie operacyjnym pojedynczej firmy / organizacji
- Masowe niszczenie aktywów firmy / grupy firm, podważanie zaufania, zagrożenie dla egzystencji firmy
- Ingerencja w działania rządu lub ważnych ogniw infrastruktury kraju

Cyberbezpieczeństwo

Przykłady ataków

- Włamanie do systemu sterowania maszyny, pojazdu, aparatu medycznego, linii produkcyjnej
- Kradzież nowego filmu / płyty / gry, nielegalna sprzedaż wersji hakerskiej przed oficjalnym rozpoczęciem sprzedaży
- Włamanie do systemu urzędu skarbowego, podszywanie się pod inne osoby
- Wielkoskalowe operacje prowadzone przez agendy rządowe lub organizacje terrorystyczne
- Mój własny przykład – próba wyłudzenia płatności



Cyberbezpieczeństwo

Zadanie dla działu IT ?

- Cyberbezpieczeństwo **nie jest** kwestią czysto techniczną, do wyłącznej uwagi działu IT
- Zagrożenie cyberatakiem powinno być rozpoznawane przez zarząd tak jak każde inne zagrożenie biznesu – czyli wyliczane w pieniądzu
- Wiele cyberataków było skutecznych z powodu zaniedbań / zaniechań ludzkich; regularne szkolenie personelu w tym zakresie staje się niezbędne

Do stworzenia reguł ruchu drogowego nie potrzeba znajomości procesów spalania w cylindrze. Brak specjalistycznej wiedzy z zakresu IT nie zwalnia z obowiązku uczestnictwa w dyskusji o procedurach bezpieczeństwa w tym zakresie.

Cyberbezpieczeństwo

Czynnik ludzki

- Niezależnie czy jest to wynik braku edukacji, bezmyślności, złośliwości, niemal wszystkie przeprowadzone z sukcesem ataki cybernetyczne miały w sobie „czynnik ludzkiego błędu”. Szacuje się, że 40% ataków się powiodło wyłącznie dzięki temu.
- Firmy i organizacje muszą umieć wykreować „wewnętrzną kulturę czujności”, na wszystkich poziomach organizacji. Bez tego wszystkie firewall’e, VPN-y, skomplikowane procedury dostępu pozostaną bezużyteczne

Cyberbezpieczeństwo

Współpraca organizacji

- Organizacje biznesowe, organizacje pozarządowe etc. powinny regularnie zgłaszać postulaty, dotyczące potrzebnej legislacji. Przykład: Niemcy, Indonezja, Brazylia mają prawo, które nakazuje aby serwery zawierające wrażliwe dane korporacyjne i personalne, znajdowały się na terytorium kraju (czy to skuteczne …?)

IEC 62443

- Nie jest możliwym aby pojedyncza organizacja samodzielnie wygrywała z cyberatakami. Konieczna jest współpraca jak największej liczby zainteresowanych, wymiana doświadczeń.
  Nec Hercules contra plures, skoro atakujących jest wielu, broniących się musi być również wielu.

PHOENIX CONTACT

Cyberbezpieczeństwo

Wskazówki dla zarządu

- Regularne dyskusje na poziomie zarządu. Traktuj zagrożenie cyberatakiem jak każde inne ryzyko biznesowe.
- Które aktywa są najbardziej narażone ? Które ryzyka są do uniknięcia ? Do zaakceptowania ? Które zagrożenia można ograniczyć ? Które można ubezpieczyć ?
- Zrozumienie skutków prawnych cyberataku dla nas, dla klientów, dla dostawców, dla pracowników
- Stworzenie i wdrożenie planu działania na wypadek cyberataku, sformułowanego prostym językiem, zrozumiałym dla wszystkich. Działać będzie wyłącznie system reagowania, działania izolowane są bez sensu

Zagrożenie atakiem cybernetycznym jest **wojną** a nie pojedynczą bitwą, która można wygrać i o niej zapomnieć. Lub inaczej mówiąc jest to **maraton** a nie sprint

Jeżeli chcielibyśmy absolutnego bezpieczeństwa, musielibyśmy wyłączyć internet. A tego przecież nigdy nie zrobimy. Musimy jednak być znacznie ostrożniejsi.
(...)
Musimy traktować komputery trochę jak samochody – opracować coś w rodzaju kodeksu drogowego dla internetu, zasady przeszkalania użytkowników, kary dla producentów za zły kod, polisy ubezpieczeniowe od szkód.

Maciej Nowicki, Newsweek, cytat z artykułu „Zimna woja internetowa”

Dziękuję za uwagę