Lekceważone wektory ataku – o czym należy pamiętać

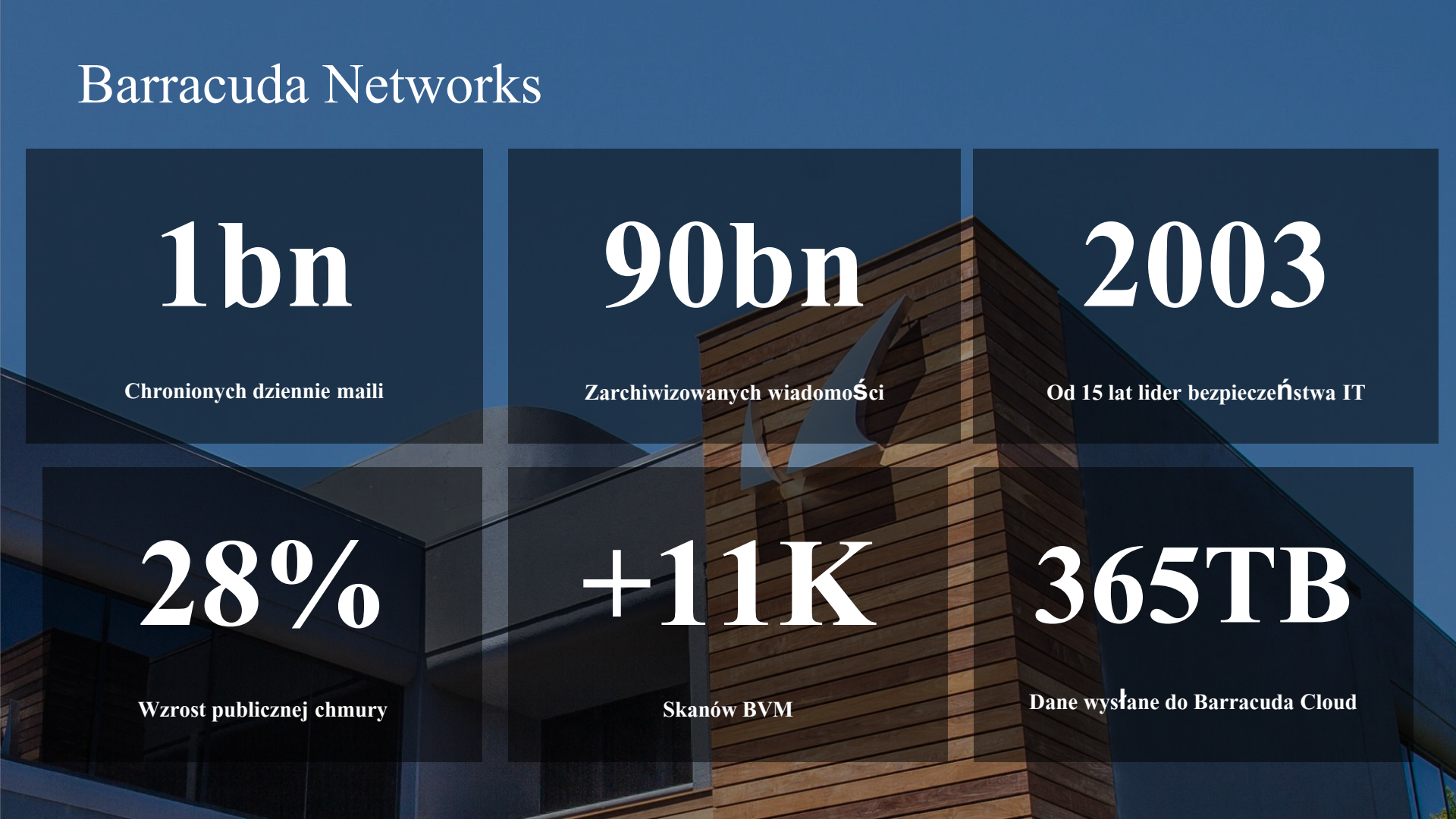
Bezpieczeństwo sieci, danych i użytkowników

Tomasz Rot
Enterprise Sales Manager

+48 507 009 507 (Mobile)
trot@barracuda.com

Barracuda

Barracuda Networks



1bn

Chronionych dziennie maili

90bn

Zarchiwizowanych wiadomości

2003

Od 15 lat lider bezpieczeństwa IT

28%

Wzrost publicznej chmury

+11K

Skanów BVM

365TB

Dane wysłane do Barracuda Cloud


Transport
PKP
POLSKIE KOLEJE PAŃSTWOWE
Spółka Akcyjna
wizzair.com
Finanse
GENERALI
FAR EAST NATIONAL BANK
遠東國民銀行
SinoPac Holdings Group Company
Handel
SWAROVSKI
CALZEDONIA
Przemysł
blum
OKT
makes life easier
Energetyka
PGNiG
OMV
Media
AGORA SA
GRUPA MEDIALNA
TVP
Administracja
MIASTO TORUŃ
Wojewódzki Sąd Administracyjny
w Gliwicach
FMCG
Kraft
MASPEX
NGO
SECOURS POPULAIRE FRANÇAIS
UNITED NATIONS
Służba zdrowia
Ministerstwo Zdrowia
tilak

NajwaŻniejsze fakty

Cyberataki są zjawiskiem powszechnym

wśród firm działających w Polsce. 82% przedsiębiorstw odnotowało przynajmniej jeden cyberincydent w 2017 roku.

37% firm odnotowało

wzrost liczby cyberataków

w przeciągu ostatniego roku (podczas gdy spadek stwierdziło tylko 5%).

Najgroźniejsze cyberzagrożenia

dla firm to: malware (APT, wycieki danych, ransomware), czynnik ludzki (kradzież danych przez pracowników, phishing) i ataki na aplikacje.

Większość firm optymistycznie ocenia dojrzałość stosowanych zabezpieczeń, czego powodem może być m.in.

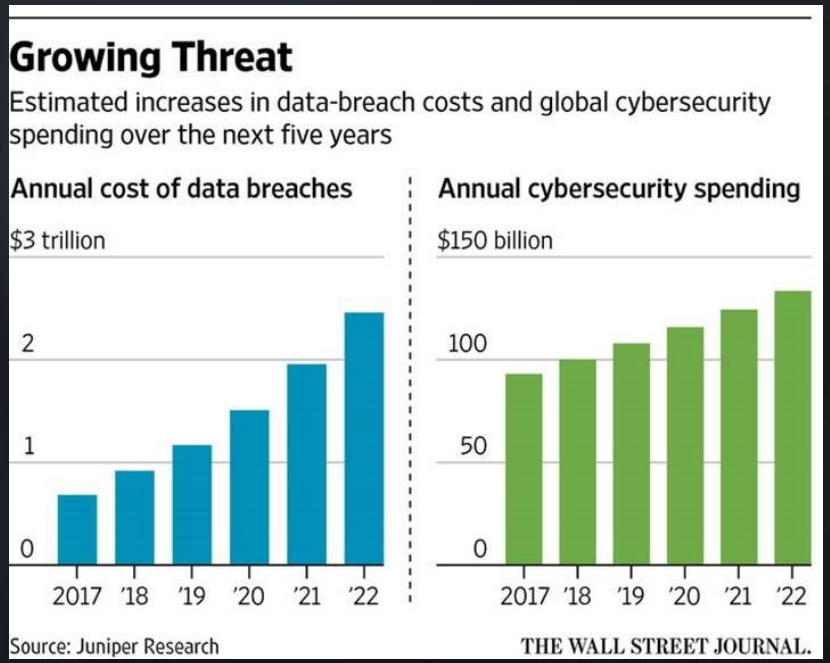
niedoszacowanie ryzyka.

Źródło : KPMG

Ile “kosztuje” nas cyberprzestępczość?

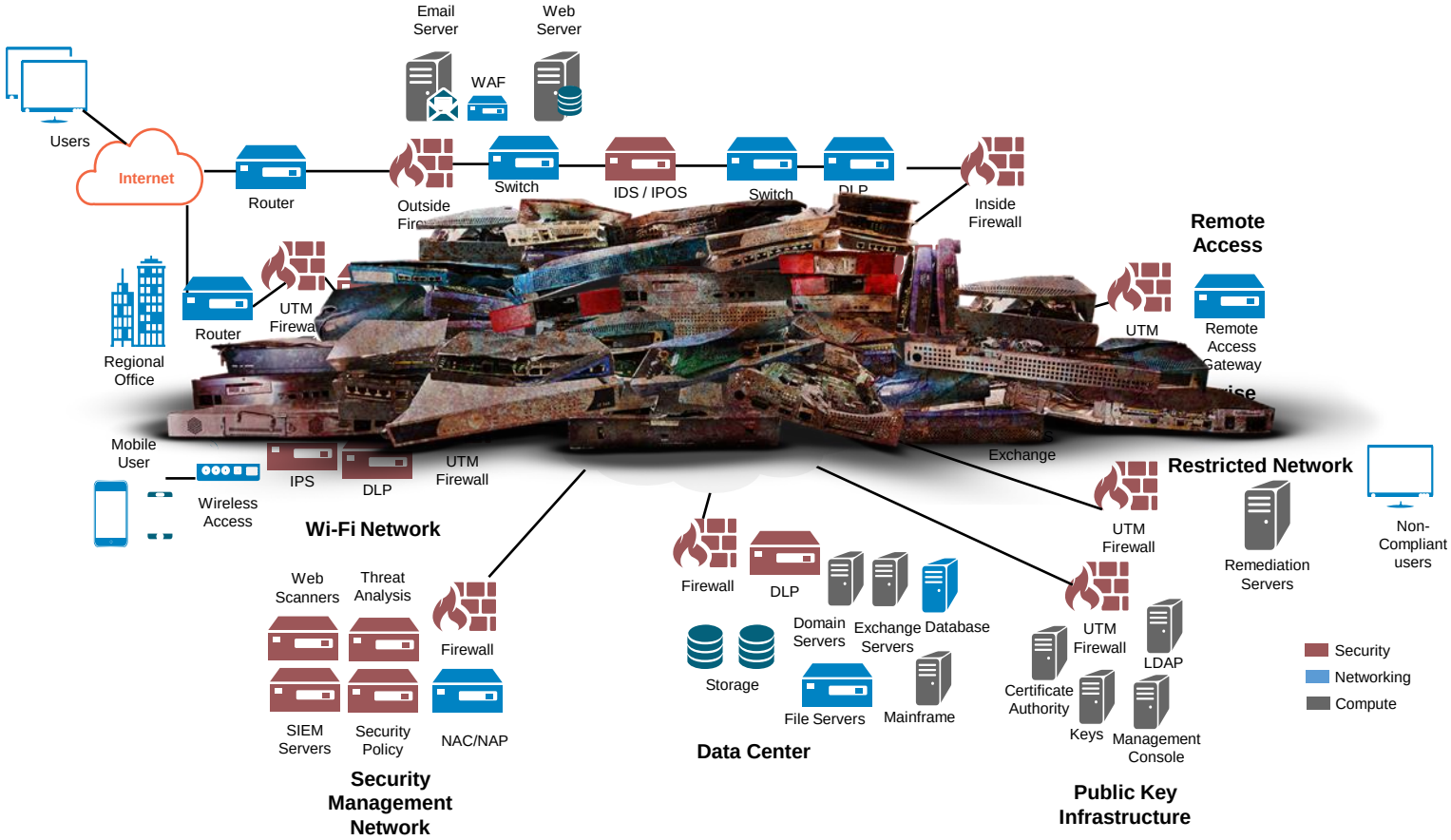
2016

Globalne wydatki na cyberbezpieczeństwo

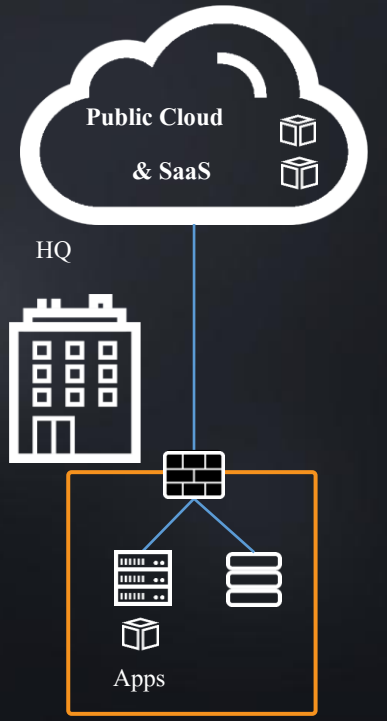


W 2022 roku globalne wydatki na bezpieczeństwo IT wyniosą ok. $ 150mld, co odpowiada mniej więcej PKB Węgier lub 1/3 PKB Polski.

Cyberekonomia – mądrze vs dużo



Wynosimy się do chmury….



Hybryda

Chmura publiczna
“All-in”

Dzielona odpowiedzialnoŚĆ (za co odpowiada dostawca usług chmurowych)

- bezpieczeństwo infrastruktury chmurowej
- jakość i dostępność platformy

- bezpieczeństwo danych
- ciągłość i bezpieczeństwo procesów

7 filarów bezpieczeństwa w chmurze

1. Wykorzystać elastyczność chmury dla ochrony ruchu sieciowego i aplikacyjnego
2. Używać tej samej metody szyfrowania danych tworzonych i przechowywanych w chmurze
3. Stosować identyczne mechanizmy kontroli tożsamości i dostępu
4. Upewnić się, że każda aplikacja chroniona jest przez zaporę aplikacyjną (WAF)
5. Zarządzać dostępem aplikacji do baz danych i informacji
6. Stale monitorować aplikacje pod kątem luk w bezpieczeństwie i podatności
7. Podwyższać i monitorować świadomość pracowników (lokalnych i zdalnych)

Miłego dnia i zapraszam do kontaktu