Myśleć jak haker?

Strategia ochrony sieci przed niektórymi atakami

Barracuda
Your journey, secured.

Kwiecień | 2019


Kim jest dzisiaj haker?

Na jakich wodach pływamy

FW
Barracuda
CloudGen Firewall

WAF
Barracuda
Web Application Firewall

WSG
Barracuda
Web Security Gateway

Barracuda
Vulnerability Manager

Bezpieczeństwo sieci i aplikacji

ESG
Barracuda
Email Security Gateway

SEN
Barracuda
Sentinel

Barracuda
Email Threat Scanner

PL
Barracuda
PhishLine

ESS
Barracuda
Essentials

MA
Barracuda
Message Archiver

Ochrona poczty

BU
Barracuda
Backup

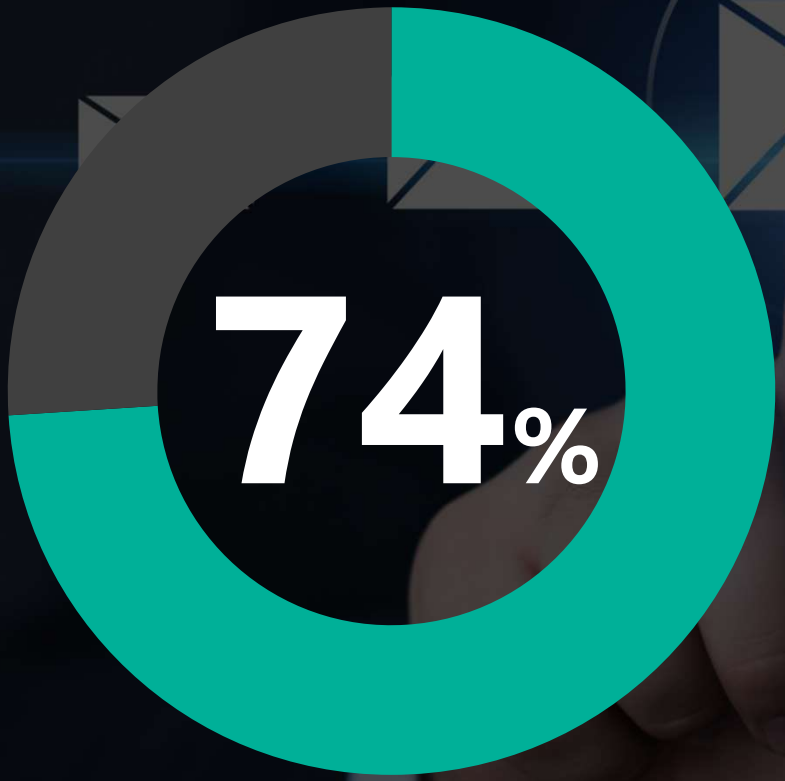
CCB
Barracuda
Cloud-to-Cloud Backup

Bezpieczństwo danych

Gartner:
__% przedsiębiorstw uważa *email*
za kluczową usługę w firmie

Gartner:
51% przedsiębiorstw uważa *email*
za kluczową usługę w firmie

Poczta pierwszym wektorem ataków

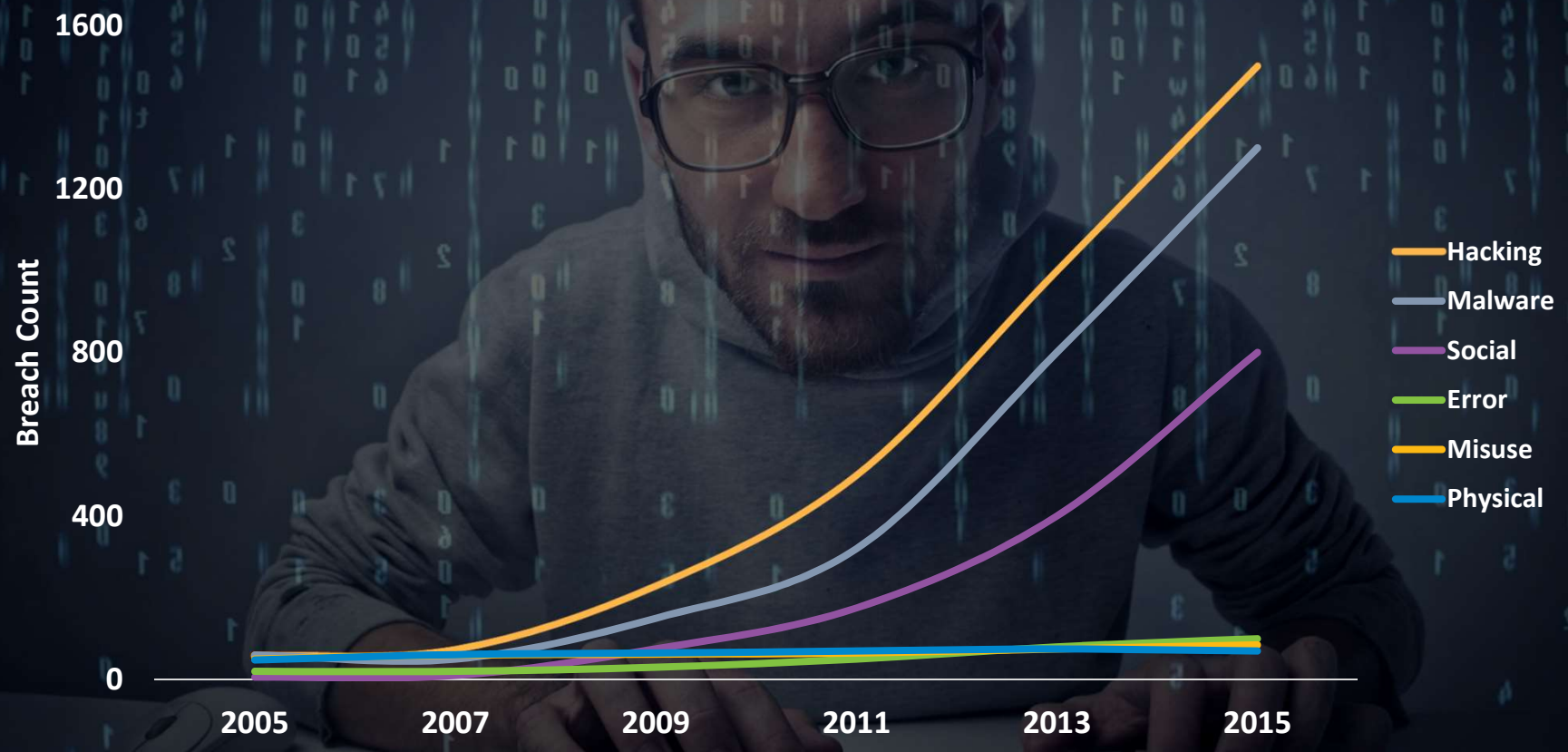


"Niemal trzy czwarte spośród wszystkich ataków rozpoczyna się od nadania wiadomości email."

- SANS Analyst Program

2017 Threat Landscape Survey: Users on the Front Line - SANS Analyst Program

Eksplozja skutecznych ataków

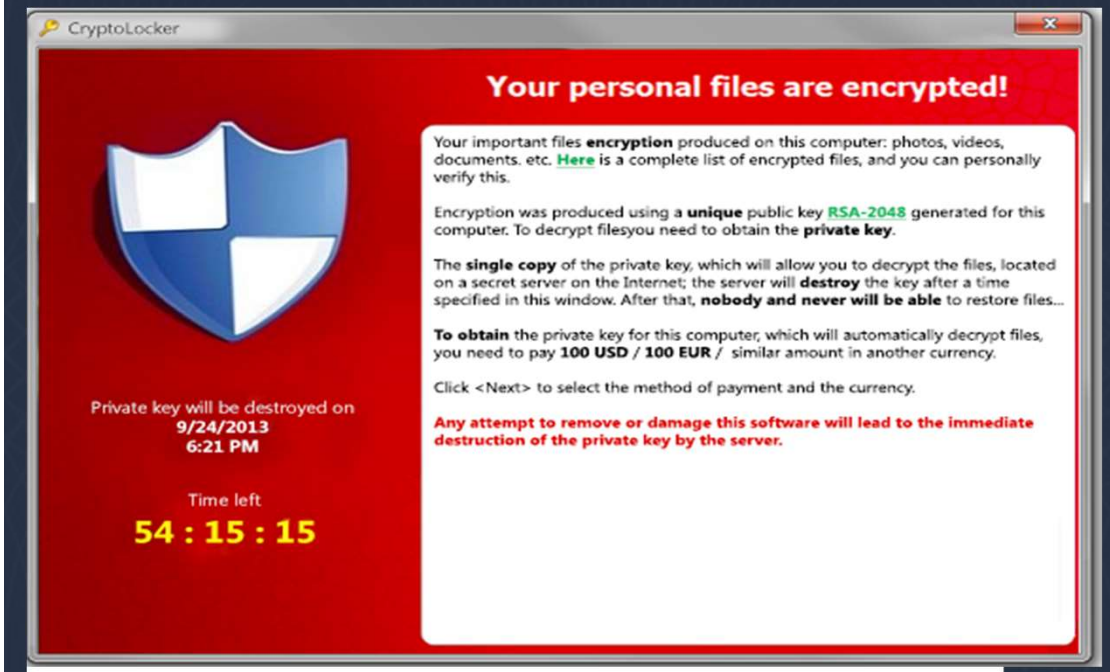


Verizon 2016 Data Breach Investigations Report

Anatomia hackingu

REKONESANS	Obserwacja celu, zbieranie informacji
PRZYGOTOWANIE	Tworzenie email i wysłanie do ofiary
PRZENIKNIĘCIE	Pracownik otwiera zainfekowany email
WYKONANIE KODU	Złośliwy kod zezwala na dostęp do sieci
PENETRACJA SIECI	Stopniowe uzyskanie dostępu do systemów
KRADZIEŻ	Kradzież poufnych danych
WYCOFANIE	Odwrócenie uwagi, zacieranie śladów, np. atak DDoS

Anatomia infekcji ransomware



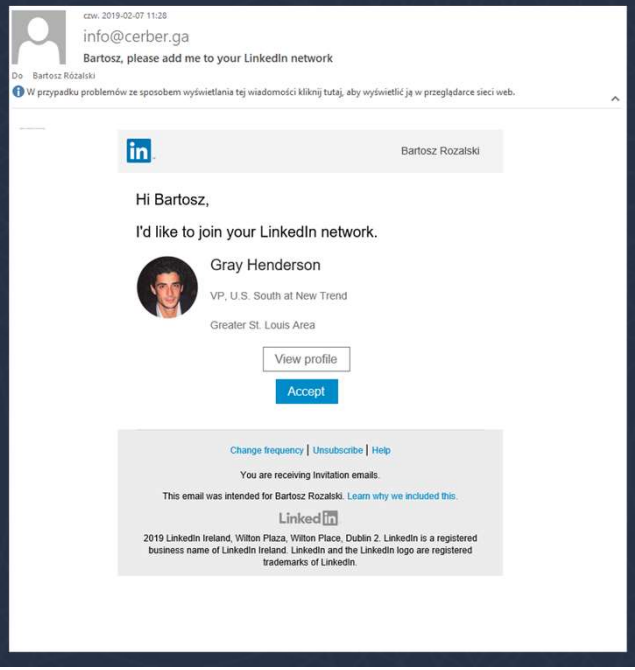
Haker wykorzystuje:

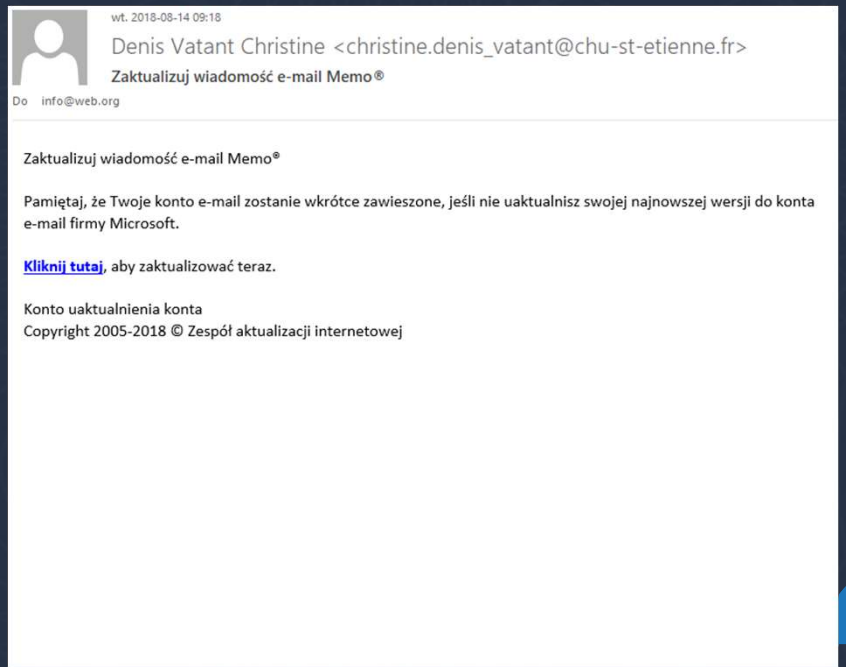
- załączniki tj. dokumenty, faktury, pliki jpeg itp.
- nakłania do kliknięcia w linki/otwarcia pliku

Anatomia spear phishingu

PHISHING — Masowe wiadomości do przypadkowych osób

SPEAR PHISHING — Spersonalizowane emaile do wybranych odbiorców (CEO,CFO)





Straty, straty, straty…

BUSINESS INSIDER POLSKA

FIRMY | FINANSE | TWOJE PIENIĄDZE | GIEŁDA | ROZWÓJ OSOBISTY

Spółka należąca do Polskiej Grupy Zbrojeniowej padła ofiarą oszustwa. Straty sięgają 4 mln zł

Business Insider Polska
8 lut, 13:07 45 016

Spółka Cenzin należąca do Polskiej Grupy Zbrojeniowej, zajmująca się handlem bronią, padła ofiarą hakerów. Pieniądze za dostawy przez kilka miesięcy przelewała na konto założone przez oszustów – dowiedziało się RMF FM. Radio informuje, że na fałszywe konto trafiło w sumie 4 mln zł.

Spółka zorientowała się, że

Niebezpiecznik
o bezpieczeństwie i nie...

SZKOLENIA | AUDYTY & PENTESTY | 10 PORAD BEZPIECZEŃSTWA |

20:05 10/2/2019

Jak ukraść miliony z polskich firm jednym e-mailem lub listem?

Autor: Piotr Konieczny | Tagi: BEC, Cenzin, e-mail, faktury, pieniądze, Polska Grupa Zbrojeniowa, socjotechnika

TVP INFO | Polska | Świat | Oglądaj na żywo | Pogoda | Nasze programy | TWOJE INFO | Więcej

Cyberatak w PGZ. Kilka milionów straty

FA, MNIE 08.02.2019, 13:50

Udostępnij:

NAJNOWSZE

- 10:09 „Górnictwo kosmiczne da oddech naszej gospodarce"
- 09:56 Zatrzymano nastolatków podejrzewanych o dewastację kalwarii w Katowicach
- 09:53 Afganistan: Co najmniej 16 zabitych w ataku na firmę budowlaną
- 09:50 Kolejne osoby zatrzymane przez CBA ws. nielegalnego wywożenia leków za granicę
- 09:47 Suski: Warto dać Polakom więcej pieniędzy
- 09:35 Zlikwidowano nielegalną fabrykę papierosów. „Straty Skarbu Państwa mogły sięgnąć 20 mln zł"

NASK | Cert PL:
40% incydentów stanowił *phishing*

Raport roczny z działalności CERT Polska 2017

Barracuda Total Email Protection

ESG

Barracuda
Email Security Gateway

Barracuda **Email Security Gateway**

Pełna ochrona serwera pocztowego

ESG

Barracuda
Email Security Gateway

Wielowarstwowe skanowanie

- Filtrowanie poczty przychodzącej/wychodzącej
- 12 warstw ochrony
- Usługa „email continuity"

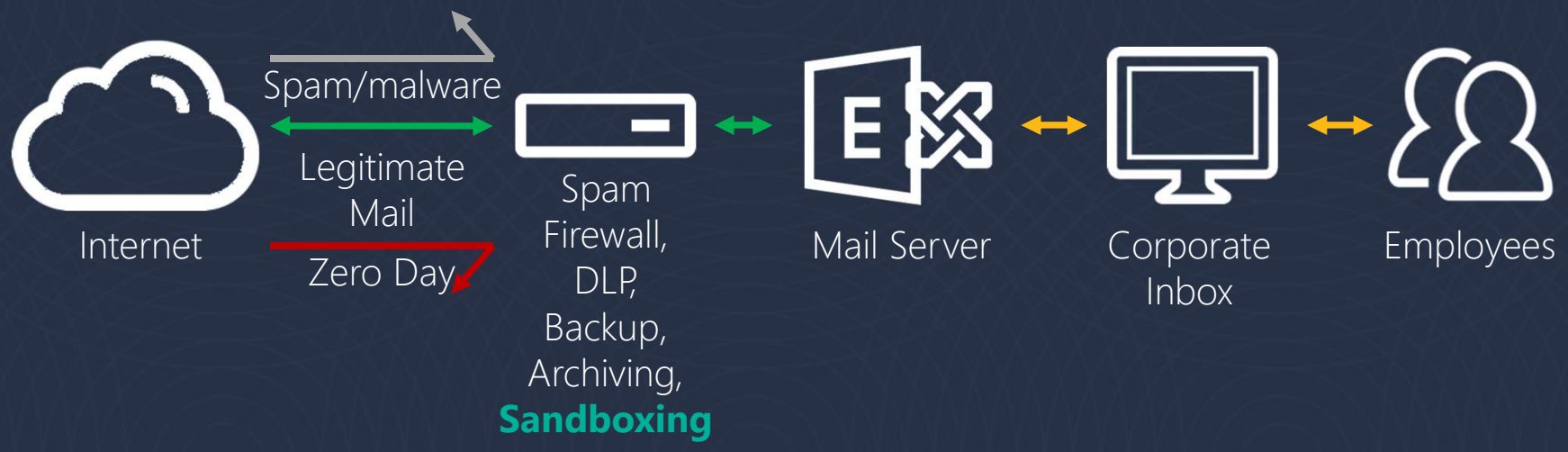
Zaawansowany sandboxing

Ochrona przed wyciekiem (DLP)

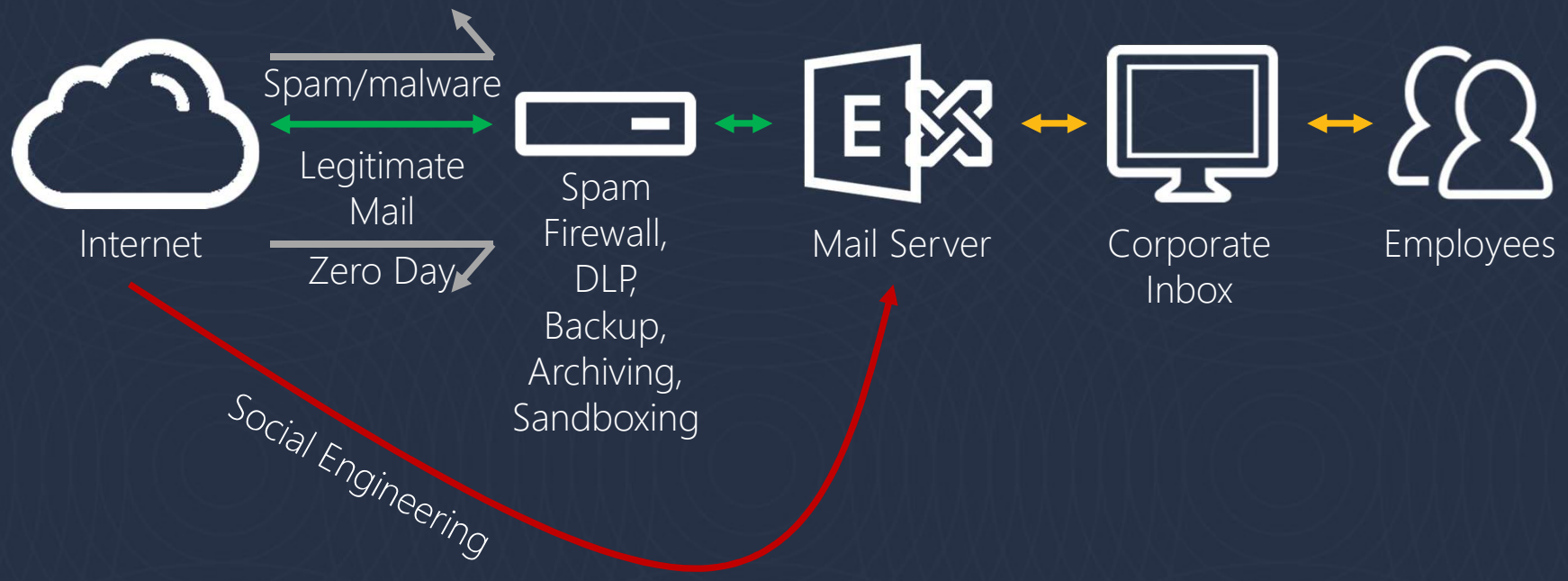
Kwarantanna per user

Pełny monitoring ruchu pocztowego

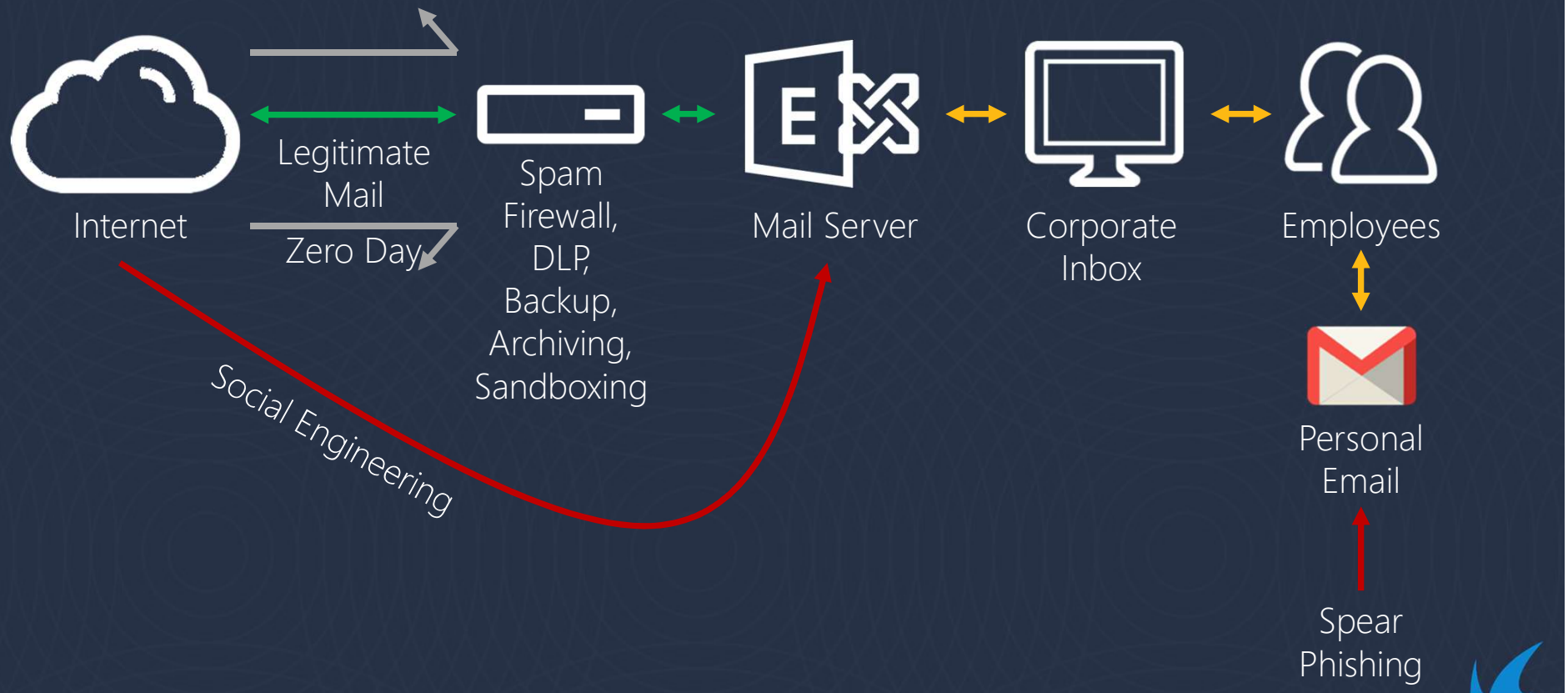
Barracuda Email Security Gateway



Ataki socjotechniczne trudne do wykrycia…



i mogą pochodzić z wnętrza sieci



SEN

Barracuda
Sentinel

Barracuda **Sentinel**

Ochrona przed wyłudzeniami

SEN

Barracuda
Sentinel

Sztuczna Inteligencja zaporą przed targetowanymi atakami

- Uczenie na ponad 2,5 mln skrzynkach email
- <1:1,000,000 współczynnik false positive
- Wykrywa ataki niedostępna dla bramy pocztowej

Wykrywa i przeciwdziała wyłudzeniom

- Ma wgląd do wzorców korespondencji
- Wyłapuje nietypowe zapytania i zgłoszenia

Ochrona marki i raportowanie DMARC

- Wgląd w próby podszywania się pod organizację

PL

Barracuda
PhishLine

Barracuda **PhishLine**

Edukacja: szkolenie i testowanie

PL

Barracuda
PhishLine

- Wzmacnia tzw. „Human firewall”
- Wbudowane wzorce gotowe do „kampanii”
- Dostarcza różne typy ataków
- Modułowe kursy i szkolenia
- Narzędzia do mierzenia efektywności

Narzędzia i dostępne materiały

Zdalne webinary techniczne i sesje techniczne

- https://www.barracuda.com/Wydarzenia

Darmowe narzędzie do Email Threat Scanner

- https://scan.barracuda.com

30-dniowe testy

- https://www.barracuda.com.pl/Testuj

CloudGeneration Firewall

Barracuda
Your journey, secured.


Dziękujemy!!!
Barracuda
Your journey, secured.