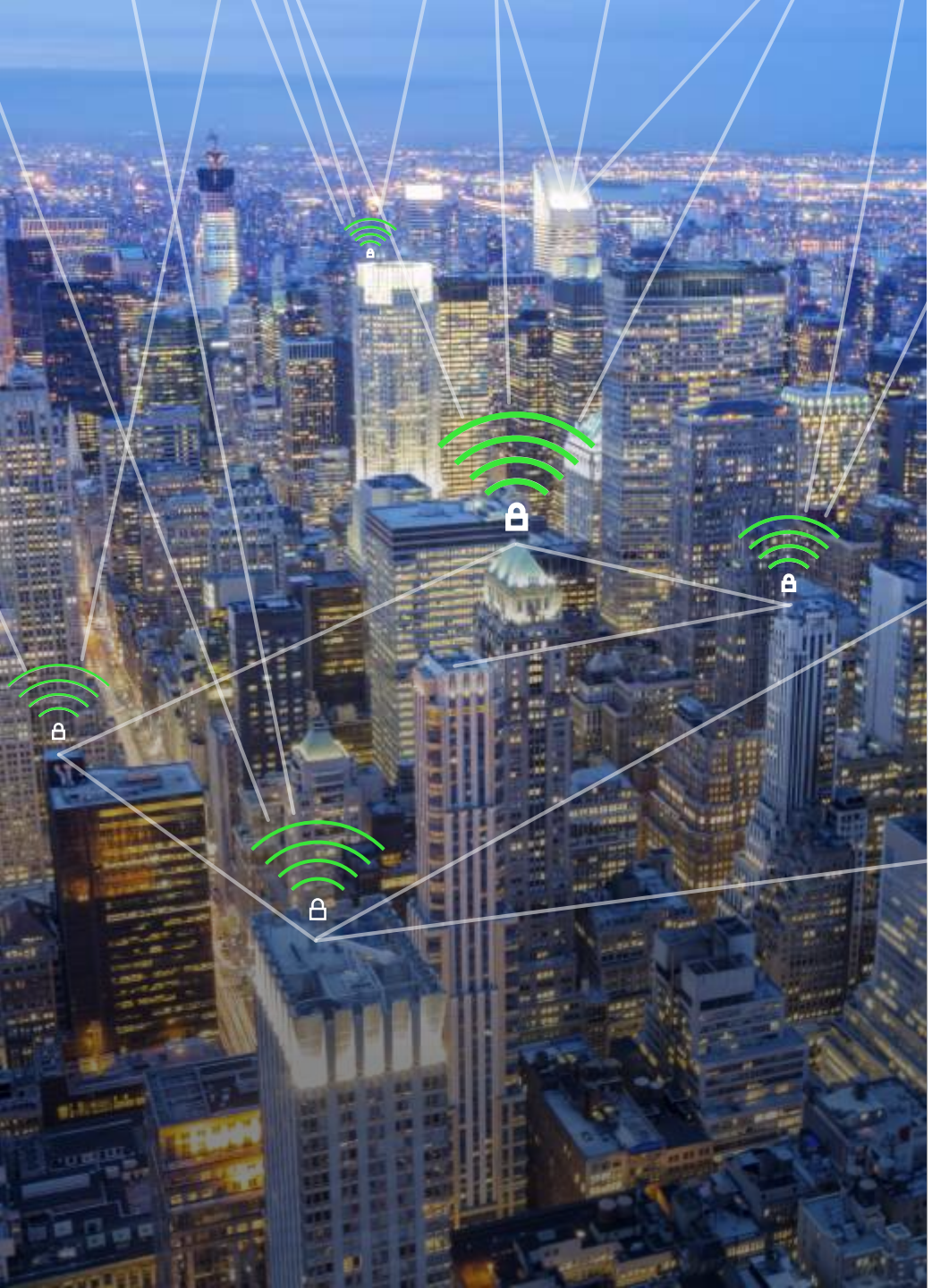
Microsoft

Cyberbezpieczna fortyfikacja XXI wieku, czyli jak Microsoft chroni Azure'a?



- Kiedy chmura się opłaca?
- Cyfrowa fortyfikacja XXI wieku
- Rok do RODO

Sylwia Stefaniak

House of Cloud Project Manager

at Microsoft

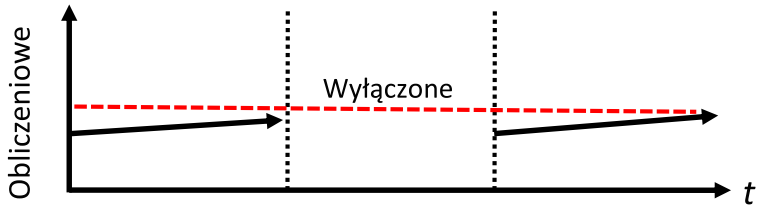
Olga Budziszewska

Cybersecurity Assurance Program Manager

at Microsoft

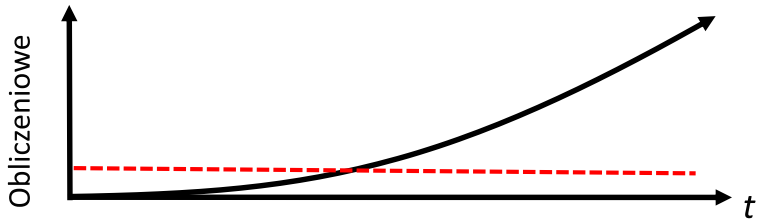
Kiedy chmura się opłaca?

Opłaca się gdy…



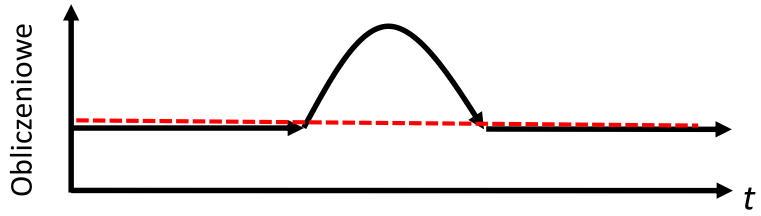
Włącz-wyłącz

Gotowe rozwiązanie do użycia w każdej chwili



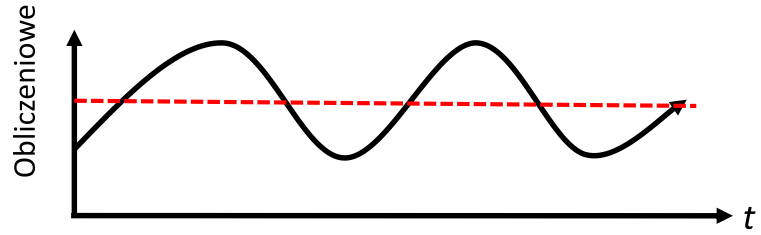
Szybki wzrost

„Ofiara własnego sukcesu”



Nieprzewidywalne

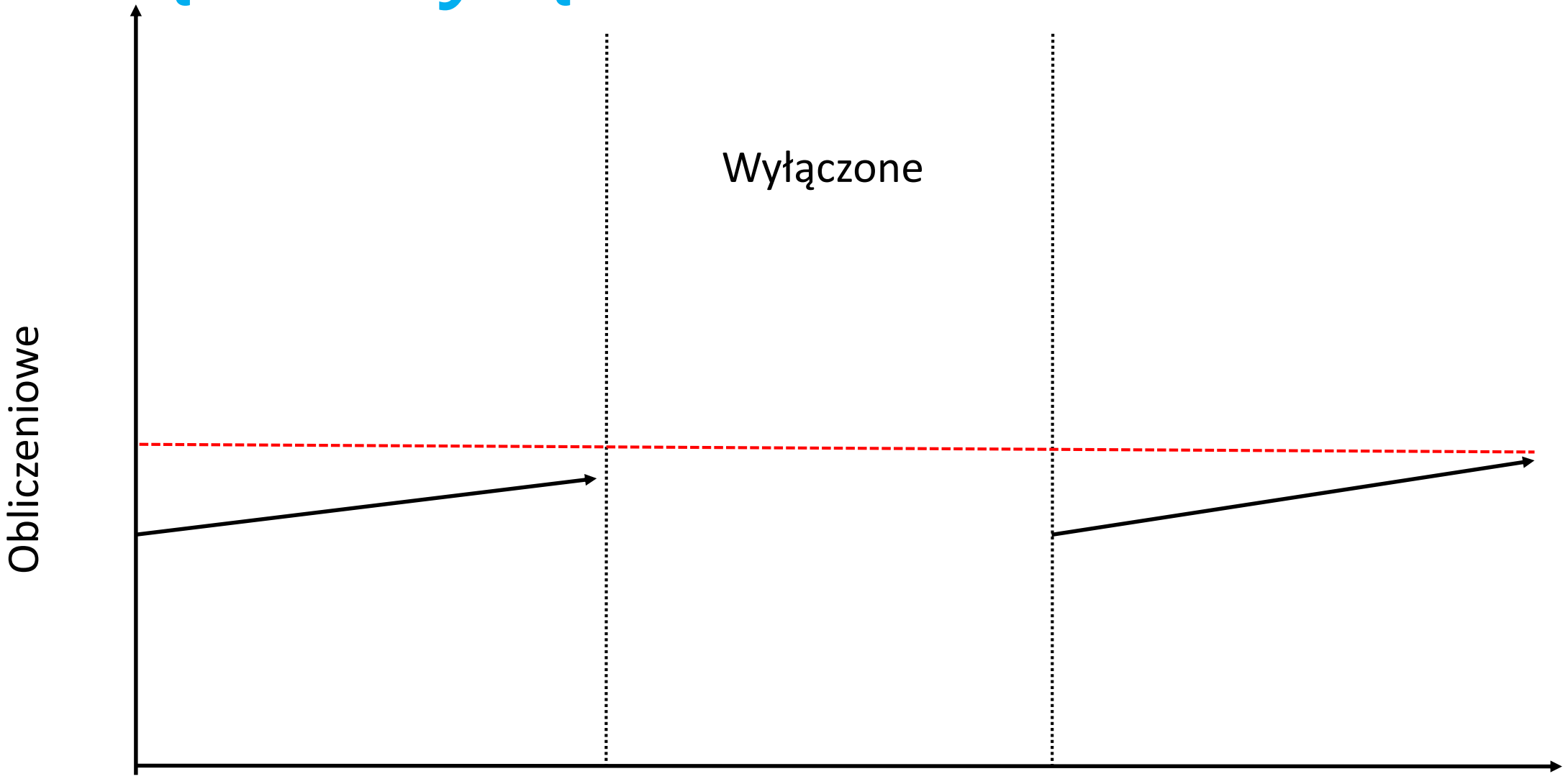
„Z zaskoczenia”



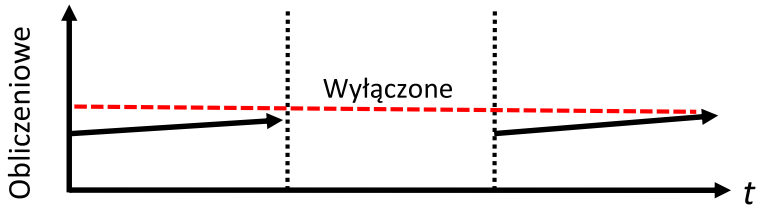
Przewidywalne

„roller coaster”

Włącz-wyłącz

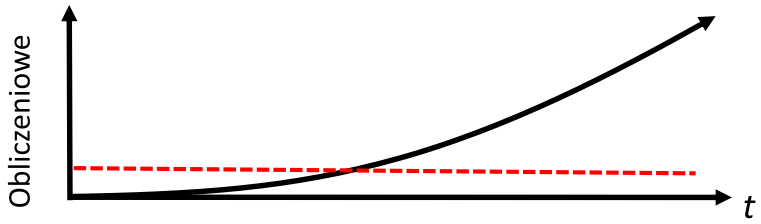


Opłaca się gdy…



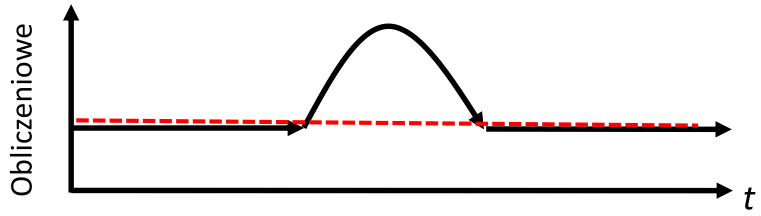
Włącz-wyłącz

Gotowe rozwiązanie do użycia w każdej chwili



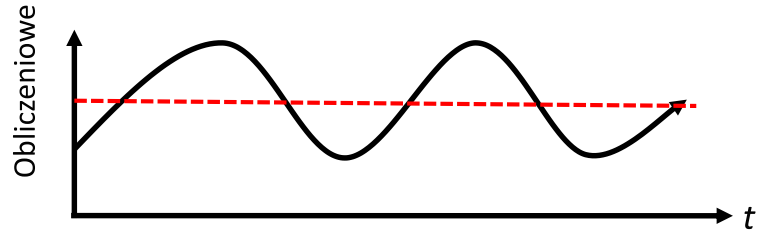
Szybki wzrost

„Ofiara własnego sukcesu”



Nieprzewidywalne

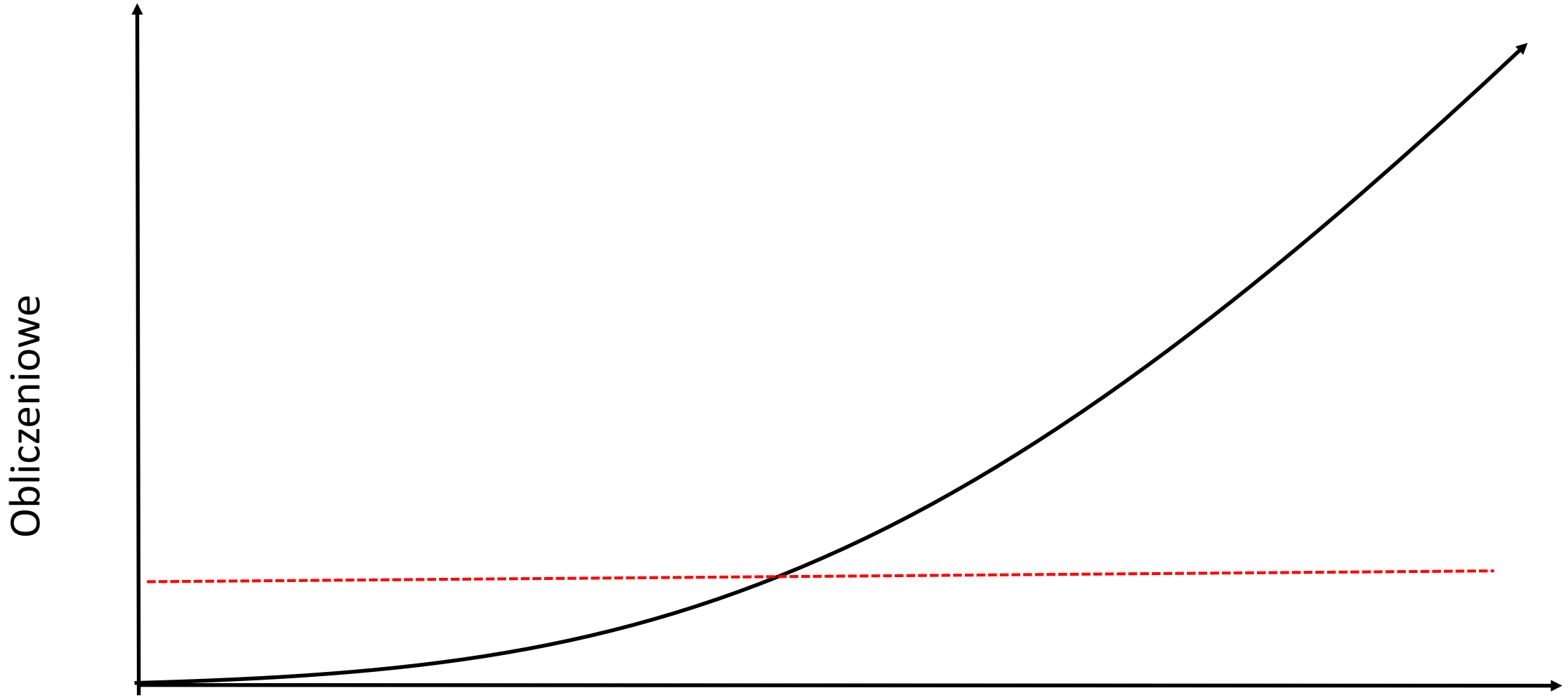
„Z zaskoczenia”



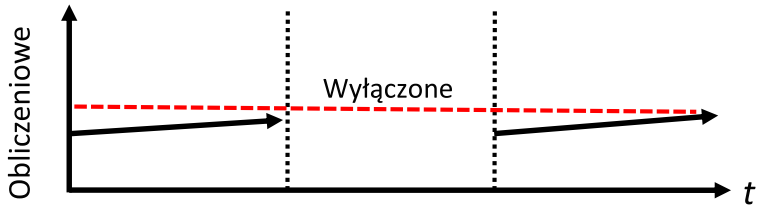
Przewidywalne

„roller coaster”

Szybki wzrost

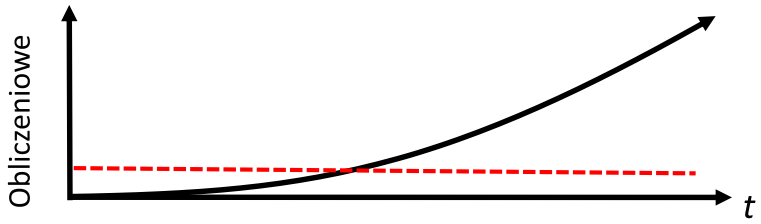


Opłaca się gdy…



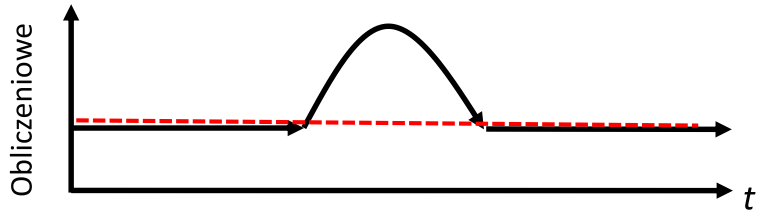
Włącz-wyłącz

Gotowe rozwiązanie do użycia w każdej chwili



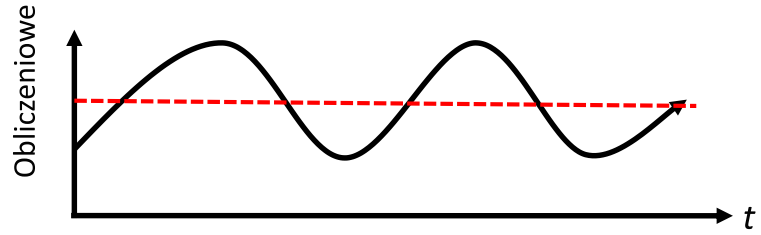
Szybki wzrost

„Ofiara własnego sukcesu”



Nieprzewidywalne

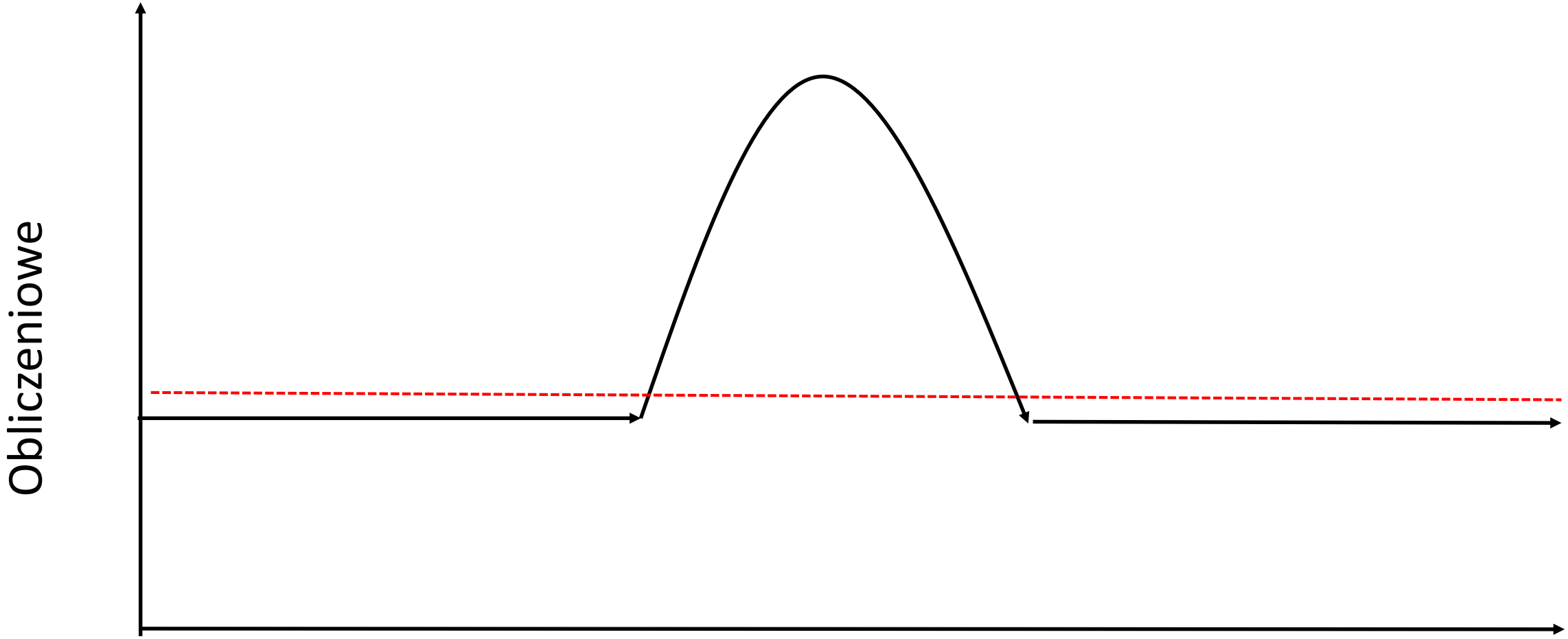
„Z zaskoczenia”



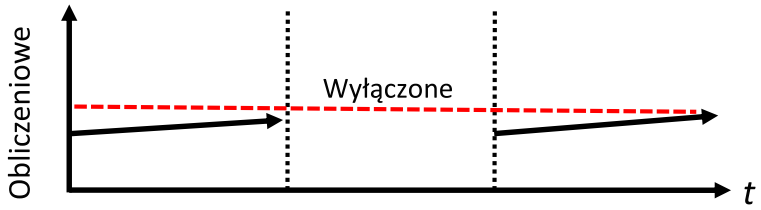
Przewidywalne

„roller coaster”

Nieprzewidywalne

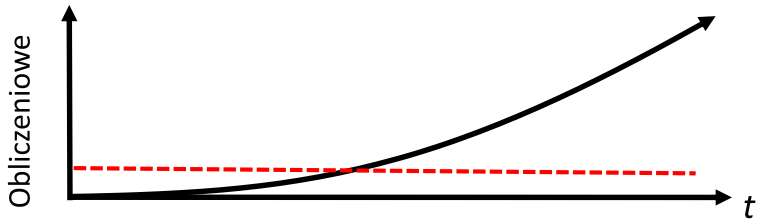


Opłaca się gdy…



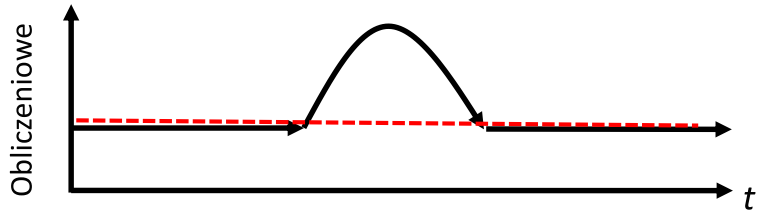
Włącz-wyłącz

Gotowe rozwiązanie do użycia w każdej chwili



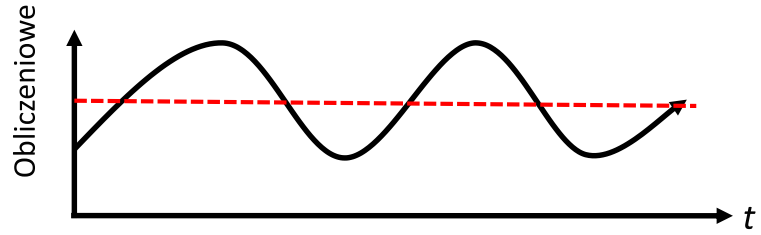
Szybki wzrost

„Ofiara własnego sukcesu”



Nieprzewidywalne

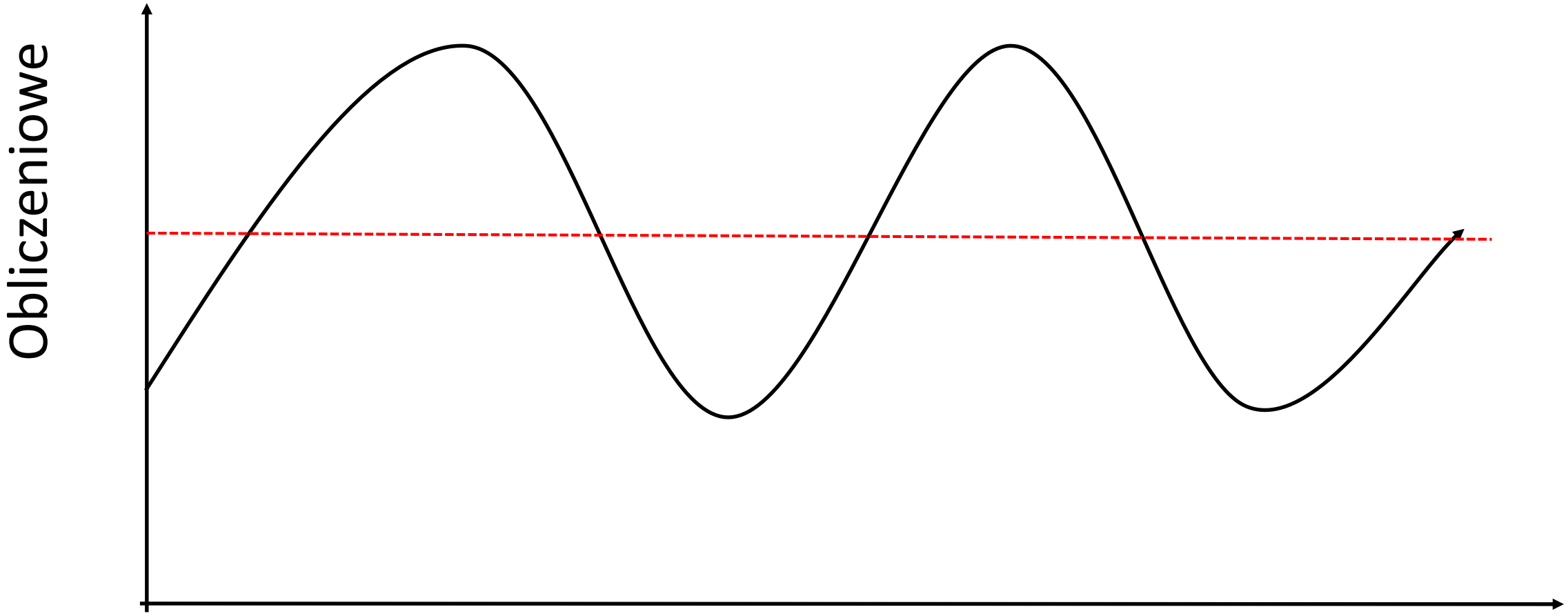
„Z zaskoczenia”



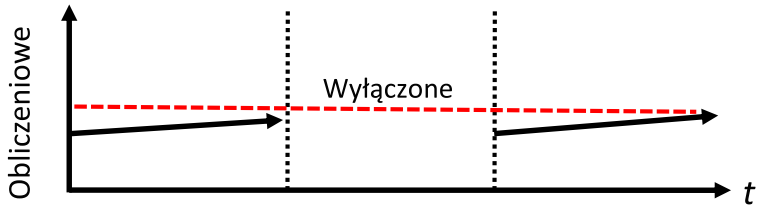
Przewidywalne

„roller coaster”

Przewidywalne

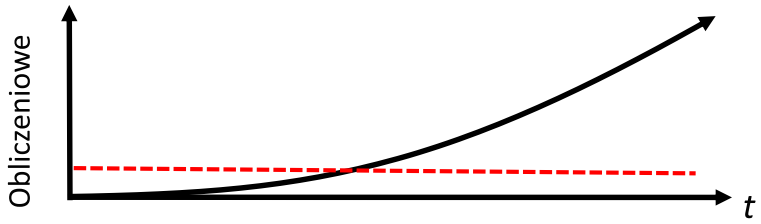


Opłaca się gdy…



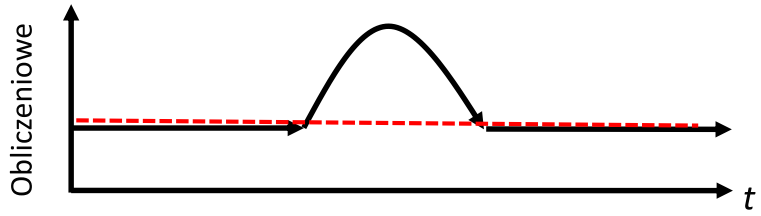
Włącz-wyłącz

Gotowe rozwiązanie do użycia w każdej chwili



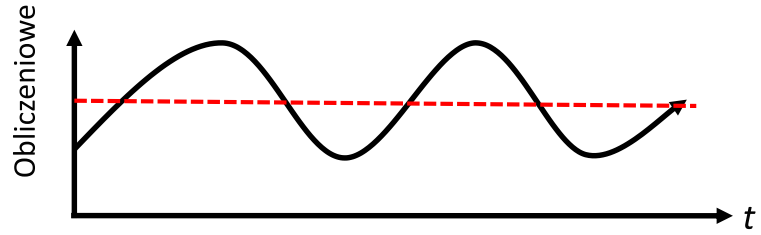
Szybki wzrost

„Ofiara własnego sukcesu”



Nieprzewidywalne

„Z zaskoczenia”



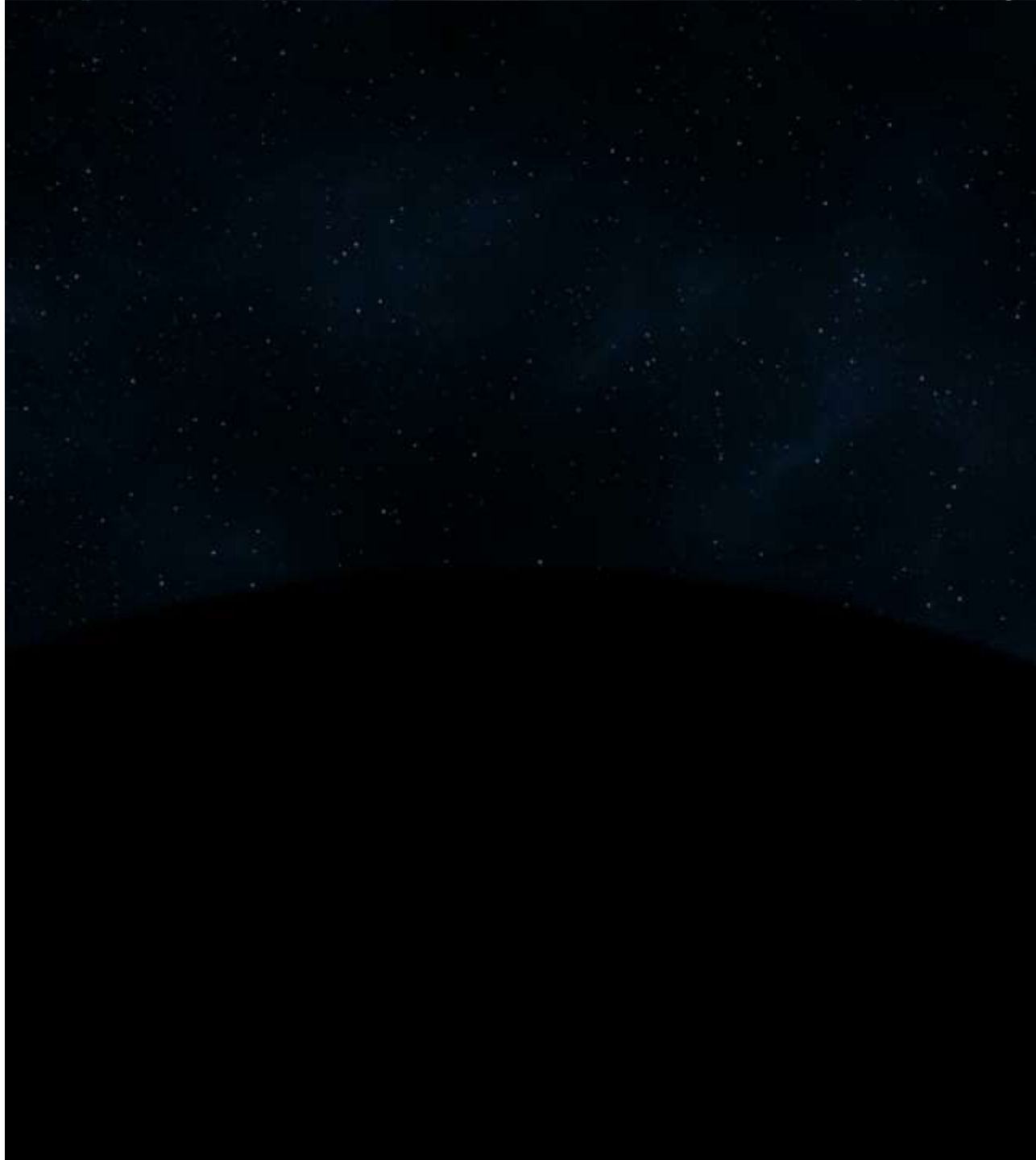
Przewidywalne

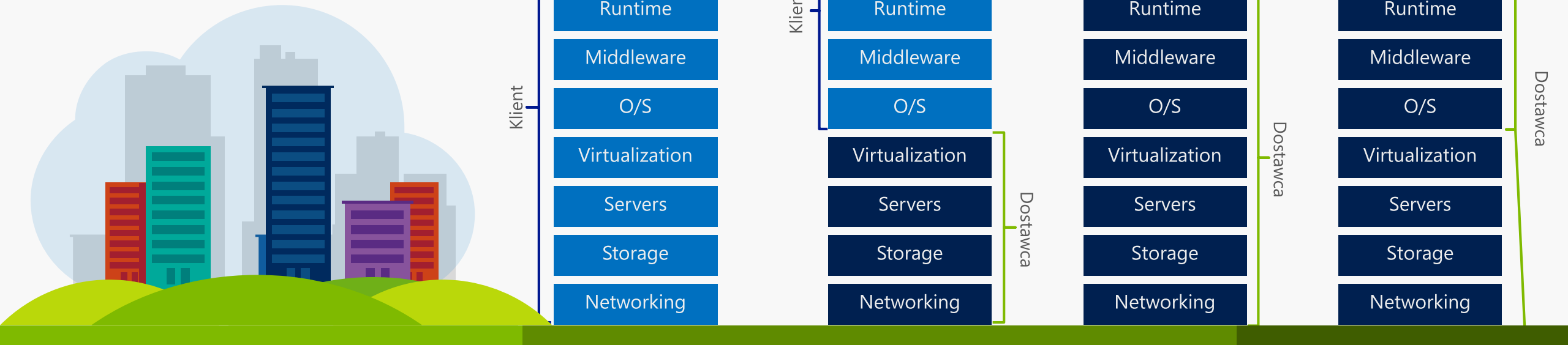
„roller coaster”

Cloud Computing w Polsce

Poland Cloud Services Market 2016–2020 Forecast and 2015 Vendor Shares

Dlaczego chmura?




Model Tradycyjny
Infrastuktura jako usługa
Platforma jako usługa
Oprogramowanie jako usługa
Data
Applications
Runtime
Middleware
O/S
Virtualization
Servers
Storage
Networking
Klient
Dostawca

Różnorodność **rozwiązań** i współdzielenie **odpowiedzialności**

Model Tradycyjny

Klient

- Data
- Applications
- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking

Microsoft Azure

Infrastuktura jako usługa

Klient

- Data
- Applications
- Runtime
- Middleware
- O/S

Dostawca

- Virtualization
- Servers
- Storage
- Networking

Platforma jako usługa

Klient

- Data
- Applications

Dostawca

- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking

Oprogramowanie jako usługa

Dostawca

- Data
- Applications
- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking


NORSE
450 000 000 000
ATTACK ORIGINS
COUNTRY
520 United States
216 China
112 Netherlands
41 Ukraine
20 Czech Republic
19 Germany
18 South Korea
18 Switzerland
17 India
ATTACK TYPES
PORT SERVICE TYPE
421 25 smtp
184 23 telnet
143 5900 rfb
85 8080 http-alt
42 3389 ms-wbt-server
29 445 microsoft-ds
28 50864 xsan-filesystem
18 123 ntp
18 53413 netis-router
ATTACK TARGETS
COUNTRY
740 United States
278 United Arab Emira...
24 Italy
24 Spain
19 France
11 Norway
10 Saudi Arabia
8 Belgium
6 Thailand
LIVE ATTACKS
TIMESTAMP ATTACKER ATTACKER IP ATTACKER GEO TARGET GEO ATTACK TYPE PORT
21:12:57.691 Superservers Llc 185.103.109.119 Vila Nova De G... De Kalb Junctio... rfb 5900
21:12:57.211 Microsoft Corporation 207.46.100.247 Redmond, US De Kalb Junctio... smtp 25
21:12:56.688 Microsoft Corporation 65.55.169.248 Washington, US De Kalb Junctio... smtp 25
21:12:56.211 Microsoft Corporation 207.46.100.252 Redmond, US De Kalb Junctio... smtp 25
21:12:55.733 Zhenjiang Sky Netbar 218.3.55.177 Zhenjiang, CN Madrid, ES telnet 23
21:12:55.732 Zhenjiang Sky Netbar 218.3.55.177, Zhenjiang, CN Madrid, ES telnet 23
21:12:55.392 Chinanet Guangdong Province Network 113.84.21.55 Guangzhou, CN Lynnwood, US xsan-filesystem 50864
21:12:54.971 China Unicom Henan Province Network 202.102.224.68 Zhengzhou, CN Lynnwood, US unknown 49544
HOME
EXPLORE
WHY NORSE?

Trusted Cloud Day
16/11/2016

MARUTA \ KANCELARIA RADCÓW PRAWNYCH

ODPOWIEDZIALNOŚĆ

Osobowa:

- Karna ogólna
- Karna za utrudnianie (NIK, GIODO, KNF, Policja, ABW, CBA, ETC)
- Pracownicza

Instytucjonalna:

- Administracyjna
- Cywilna: **(i)** deliktowa, **(ii)** za produkt (np. oprogramowanie), oraz **(iii)** kontraktowa
- Reputacyjna
- Podmiotów zbiorowych (karna)

Microsoft

Trusted Cloud Day
16/11/2016

MARUTA \ KANCELARIA RADCÓW PRAWNYCH

PRZYKŁAD ZARZUTU

art. 52 UODO (niezabezpieczenie) w zbiegu z
art. 23 ust. 1 UZNK (tajemnica przedsiębiorstwa) w zbiegu z
art. 266 § 1 KK (tajemnica służbowa) w zbiegu z
art. 171 ust. 5 Pr bankowego (tajemnica bankowa) w zbiegu z
art. 296 § 1 (tajemnica służbowa) i §2 KK w związku z
art. 11§ 2 KK w związku z
art. 12 KK

Microsoft

Cyfrowa fortyfikacja XXI wieku

4 fundamentalne zasady zaufania w chmurze

> "Businesses and users are going to embrace technology only if they can trust it."
>
> **Satya Nadella, Microsoft CEO**

ZABEZPIECZENIA

Moje dane są odpowiednio chronione – i technicznie i organizacyjnie

PRYWATNOŚĆ

Moje dane należą do mnie i to ja chcę je kontrolować

ZGODNOŚĆ

Chcę mieć pewność i gwarancje, że dostawca chmury stosuje te środki

JAWNOŚĆ

Chcę wiedzieć, w jaki sposób dostawca przechowuje moje dane

Microsoft

Globalna skala, lokalny dostęp

38
Regionów

140
Państw świata

200+
Usług online

Cybernetyczna fortyfikacja | Centrum Danych Microsoft

powierzchnia ponad 6,5 ha

20 000 m^3 betonu

3400 ton stali

ponad 300 km traktów

2400 tony miedzi

12 km wodnej instalacji chłodzącej

moc pobierana do 60 MW

wartość inwestycji: **$500M+**

Cybernetyczna fortyfikacja | jak Microsoft zabezpiecza swoje centra danych?

24x7x365

monitorowanie i rejestrowanie

brak uprawnień ponadstandardowych

izolacja

ochrona przed złośliwym oprogramowaniem

wykrywanie włamań i ataków DDoS

komunikacja szyfrowana

tożsamość i dostęp

Chmura godna zaufania

GLOBALNE

- ISO 27001
- ISO 27018
- ISO 27017
- ISO 22301
- SOC 1 Type 2
- SOC 2 Type 2
- SOC 3
- CSA STAR Self-Assessment
- CSA STAR Certification
- CSA STAR Attestation

USA

- Moderate JAB P-ATO
- High JAB P-ATO
- DoD DISA SRG Level 2
- DoD DISA SRG Level 4
- SP 800-171
- FIPS 140-2
- Section 508 VPAT
- ITAR
- CJIS
- IRS 1075

PRZEMYSŁOWE

- PCI DSS Level 1
- CDSA
- MPAA
- FACT UK
- Shared Assessments
- FISC Japan
- HIPAA / HITECH Act
- HITRUST
- GxP 21 CFR Part 11
- MARS-E
- IG Toolkit UK
- FERPA
- GLBA
- FFIEC

REGIONALNE

- Argentina PDPA
- EU Model Clauses
- UK G-Cloud
- China DJCP
- China GB 18030
- China TRUCS
- Singapore MTCS
- Australia IRAP/CCSL
- New Zealand GCIO
- Japan My Number Act
- ENISA IAF
- Japan CS Mark Gold
- Spain ENS
- Spain DPA
- India MeitY
- Canada Privacy Laws
- Privacy Shield
- Germany IT Grundschutz workbook

Cybernetyczna fortyfikacja

$15B+

INWESTYCJA W BUDOWĘ INFRASTRUKTURY CHMUROWEJ

1989

POWSTAJE PIERWSZE CENTRUM DANYCH W REDMOND

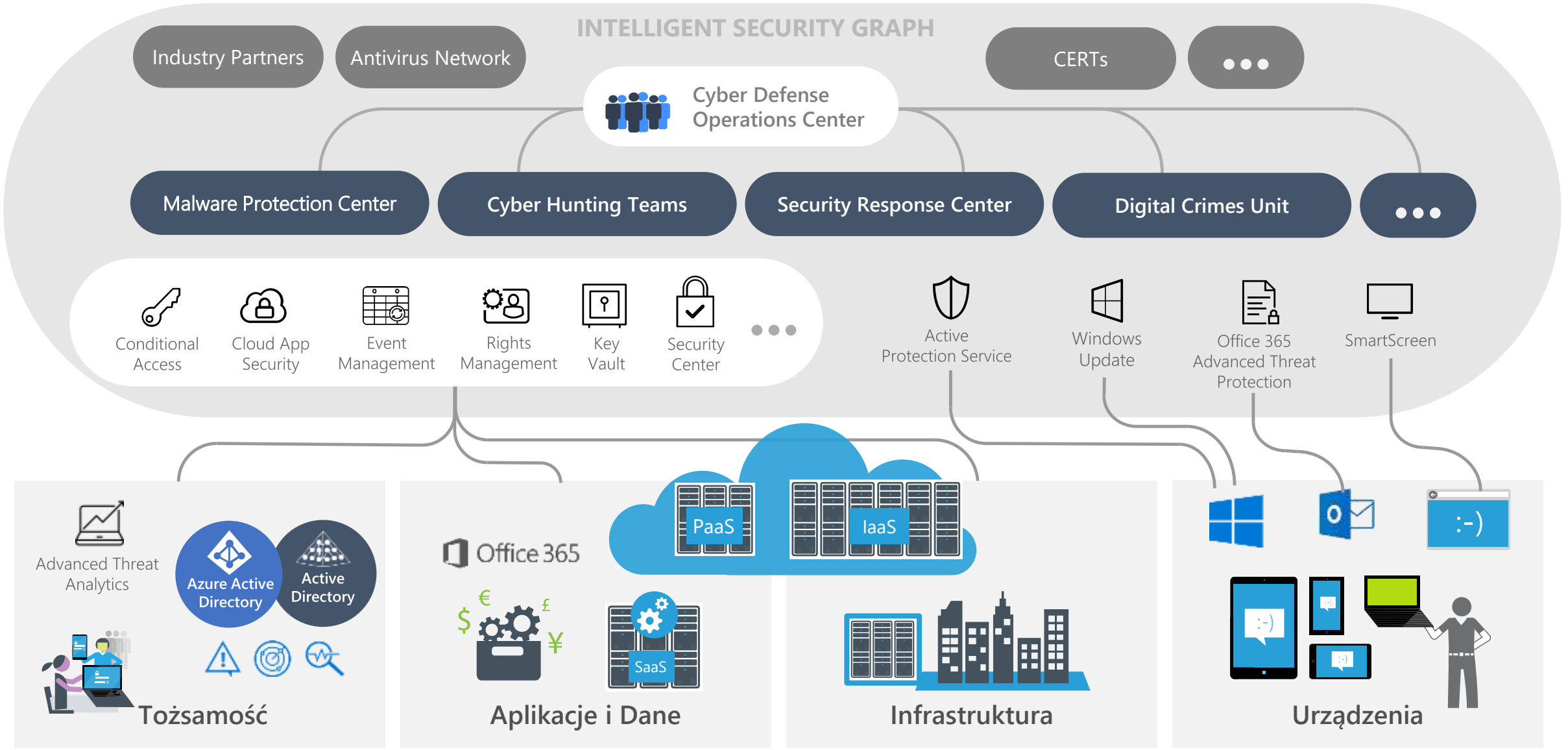
10

BOISK FUTBOLOWYCH ZMIEŚCI SIĘ W CENTRUM DANYCH W CHICAGO

3x

DŁUGOŚĆ ŚWIATŁOWODU POKONA TRASĘ NA KSIĘŻYC I Z POWROTEM

Bezpieczeństwo to proces....



Zapewnienie przejrzystości i spójności w zakresie ochrony danych osobowych w UE

General Data Protection Regulation (GDPR) wprowadza nowe zasady ochrony danych osobowych w organizacjach, które oferują towary i usługi dla obywateli Unii Europejskiej (UE) lub dla takich, które zbierają i analizują dane powiązane z obywatelami UE – nieważne gdzie te organizacje się znajdują.

- **Rozszerzenie** praw prywatości
- **Rozszerzone** obowiązki ochrony danych
- **Obowiązkowe** zgłaszanie naruszeń
- **Znaczące** kary za niezgodność z prawem

Jakie są główne zmiany związane z wejściem GDPR?

Prywatność

Osoby prywatne mają prawo do:

- Dostępu do swoich danych osobowych
- Poprawy błędów w danych osobowych
- **Usunięcia danych osobowych**
- Sprzeciwu w kontekście przetwarzania danych osobowych
- Przeniesienia danych osobowych

Kontrole i powiadomienia

- Rygorystyczne wymogi bezpieczeństwa
- **Obowiązek powiadamiania o naruszeniu**
- **Odpowiednie sformułowanie zgody na przetwarzanie danych osobowych**
- Poufność
- Ewidencjonowanie

Przejrzyste zasady

Przejrzyste i łatwo dostępne strategie dotyczące:

- Zawiadomienia o zbieraniu danych
- Zawiadomienia o przetwarzaniu
- Szczegółów przetwarzania
- Przechowywania / usuwania danych

Technologia i szkolenia

Konieczność inwestycji:

- Szkolenia pracowników i osób związanych z ochroną danych
- Wdrożenie polityk przetwarzania danych
- Inspektor Ochrony Danych
- Umowy z procesorami danych / dostawcami usług

Zobowiązanie Microsoft w stosunku do swoich

Get GDPR compliant with the Microsoft Cloud

Posted February 15, 2017 by Brendon Lynch - Chief Privacy Officer, Microsoft

The new General Data Protection Regulation (GDPR) is the most significant change to European Union (EU) privacy law in two decades. The GDPR requires that organizations respect and protect personal data – no matter where it is sent, processed or stored. Complying with the GDPR will not be easy. To simplify your path to compliance, Microsoft is committing to be GDPR compliant across our cloud services when enforcement begins on May 25, 2018.

Źródło: https://blogs.microsoft.com/on-the-issues/2017/02/15/get-gdpr-compliant-with-the-microsoft-cloud/

ZASADY PRZETWARZANIA DANYCH – ART. 5 RODO

Zasada zgodności z prawem, rzetelności i przejrzystości

Zasada ograniczenia celu

Zasada minimalizacji danych

Zasada prawidłowości

Zasada ograniczenia przechowywania

Zasada integralności i poufności

Zasada rozliczalności

PRZEJRZYSTE ZASADY: ZGODA NA PRZETWARZANIE
PKT. (42), (43) RODO

(42) Jeśli przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą, **administrator powinien być w stanie wykazać**, że osoba, której dane dotyczą, wyraziła zgodę na operację przetwarzania.

W szczególności w przypadku pisemnego oświadczenia składanego w innej sprawie powinny istnieć gwarancje, że osoba, której dane dotyczą, jest **świadoma wyrażenia zgody oraz jej zakresu.**

Zgodnie z dyrektywą Rady 93/13/EWG (1) oświadczenie o wyrażeniu zgody przygotowane przez administratora powinno mieć **zrozumiałą i łatwo dostępną formę**, być sformułowane jasnym i prostym językiem i nie powinno zawierać nieuczciwych warunków.

Aby wyrażenie zgody było świadome, osoba, której dane dotyczą, powinna **znać przynajmniej tożsamość administratora oraz zamierzone cele przetwarzania** danych osobowych.

Wyrażenia zgody nie należy uznawać za dobrowolne, jeżeli osoba, której dane dotyczą, nie ma rzeczywistego lub wolnego wyboru oraz nie może odmówić ani wycofać zgody bez niekorzystnych konsekwencji.

PRZEJRZYSTE ZASADY: ZGODA NA PRZETWARZANIE
PRZYKŁAD

„Administratorem danych jest FIRMA ABC z siedzibą w Warszawie, kod pocztowy 02-000, przy ul. Dowolnej 11. Dane osobowe przetwarzane są w celach związanych z przesyłaniem informacji handlowych i marketingowych drogą elektroniczną lub telefoniczną. Podanie danych osobowych jest niezbędne do realizacji ww. celów. Każda osoba ma prawo wglądu w swoje dane, możliwość ich poprawiania oraz usunięcia.”

PRZEJRZYSTE ZASADY: ZGODA NA PRZETWARZANIE
PRZYKŁAD

„Administratorem danych jest FIRMA ABC z siedzibą w Warszawie, kod pocztowy 02-000, przy ul. Dowolnej 11. **Inspektorem Ochrony danych jest Jan Kowalski, jan@kowalski.pl, +48 601 601 601.** Dane osobowe przetwarzane są w celach związanych z przesyłaniem informacji handlowych i marketingowych drogą elektroniczną lub telefoniczną. **Kategorie danych to imię, nazwisko, numer telefonu, adres e-mail. Dane nie są udostępniane innym podmiotom. Dane nie są przekazywane do państwa trzeciego. Osoba, której dane dotyczą nie podlega profilowaniu. Dane dostępne są w siedzibie Firmy ABC. Informuje się o możliwości uzyskania kopii danych. Dane osobowe będą przetwarzane do momentu wniesienia sprzeciwu wobec przetwarzania lub w chwili wygaśnięcia umowy.** Podanie danych osobowych jest niezbędne do realizacji ww. celów. Każda osoba ma prawo wglądu w swoje dane, możliwość ich poprawiania oraz usunięcia, **dostępu do danych, żądania ograniczenia przetwarzania, wniesienia sprzeciwu wobec przetwarzania, prawo do przenoszenia danych. Informuje się o prawie wniesienia skargi w zakresie przetwarzania danych do organu nadzorczego do Generalnego Inspektora Danych Osobowych w Warszawie, ul. Stawki 2.**”

ZGŁOSZENIE NARUSZENIA ORGANOWI NADZORCZEMU – ART. 33

W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, **nie później niż w terminie 72 godzin** po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

ALE CO TO JEST „NARUSZENIE”?

Art. 4. 12) „**naruszenie ochrony danych osobowych**” oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych

Jak zacząć?

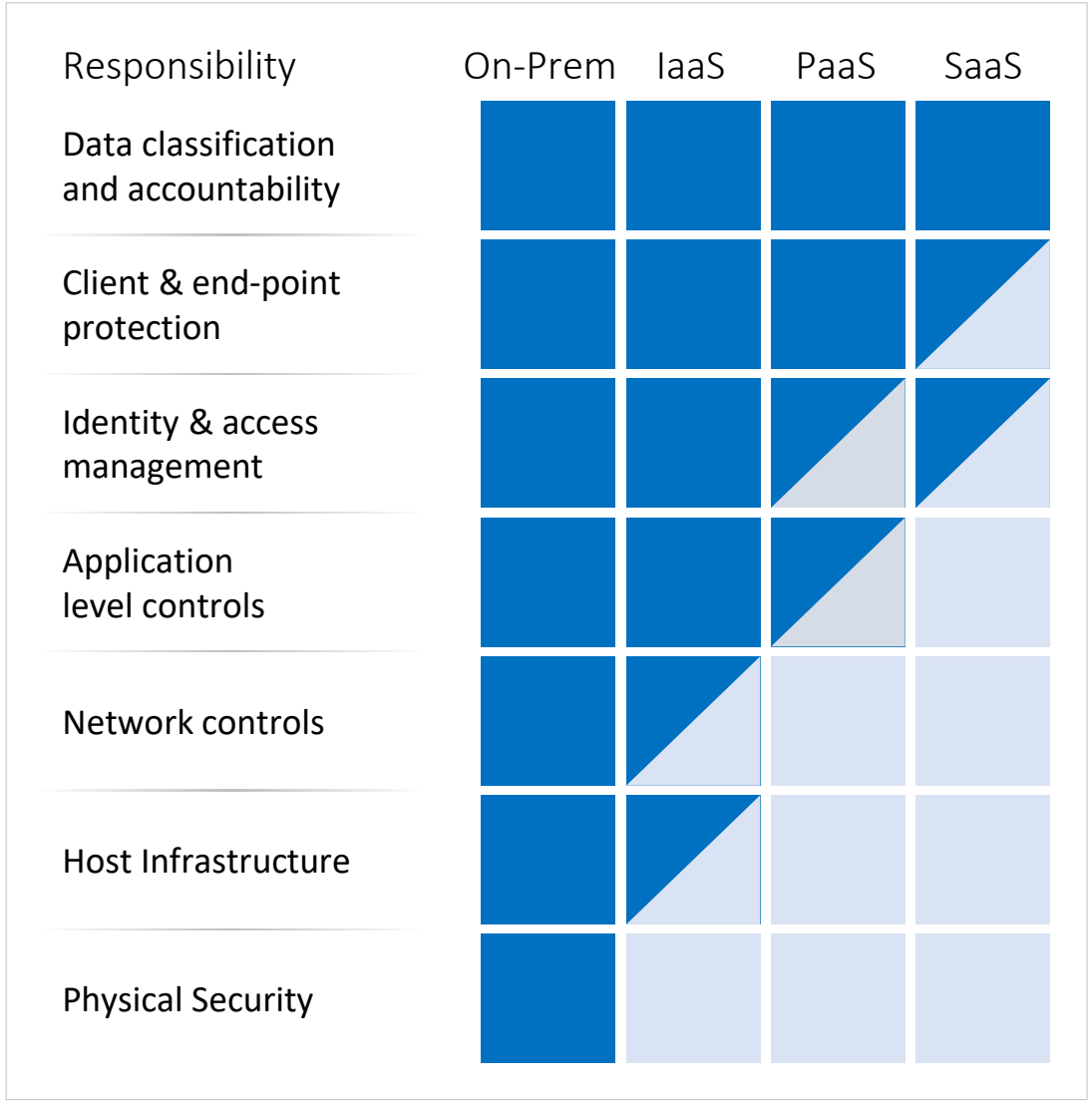
1. **Inwentaryzacja danych** – Zdefiniuj, jakie dane osobowe masz i gdzie one się znajdują
2. **Zarządzanie** – Zarządź, jak dane osobowe będą/są używane i kto może mieć do nich dostęp
3. **Ochrona** – Ustanów formy zabezpieczania do zapobiegania i wykrywania naruszeń, odpowiadania na wykryte podatności
4. **Raportowanie** – Twórz dokumentację – w szczególności na temat tego, kto ma dostęp do danych i procesów po wykryciu naruszenia

Współdzielona odpowiedzialność

Odpowiedzialność Administratora Danych

Współdzielona odpowiedzialność

Odpowiedzialność dostawcy usług



Polecam

- Wytyczne Grupy Roboczej Art. 29
  - dot. Inspektora Ochrony Danych Osobowych
  - dot. wykonania analizy ryzyka
- Webinaria Microsoft
  - https://aka.ms/gdpr1
  - https://aka.ms/gdpr2
  - https://aka.ms/gdpr3
- Microsoft.com/GDPR
- Microsoft Online Services and GDPR
  - Microsoft Azure
  - Office and Office 365
  - Microsoft Dynamics 365
  - Enterprise Mobility Suite
  - Windows and Windows Server
  - SQL Server

Olga Budziszewska

Cybersecurity Assurance Program Manager

v-olbudz@microsoft.com

Sylwia Stefaniak

House of Cloud Project Manager

v-systef@microsoft.com

Microsoft