

Above the clouds protecting Microsoft

Jelle Niemantsverdriet





Source: https://flic.kr/p/KYmnkC (Creative Commons)

Reliability?

C.

Or Trust?

It's Friday, 5pm: "We think we have a problem..."

8

A hyperscale cloud provider inherits...



Microsoft's Security Strategy

Diplomacy



Disruption



Defence



Diplomacy

Source: https://aka.ms/ukrainespecialreport - https://aka.ms/ukrainereportearlylessons - https://aka.ms/ThreatIntel-Russia

Source: https://www.politie.nl/nieuws/2023/april/5/operation-cookiemonster-nl.html https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-notorious-hacker-marketplace-selling-your-identite crimals

OPERATION COOKIE MONSTER

Genesis Market's domains have been seized by the FBI pursuant to a seizure warrant issued by the United States District Court for the Eastern District of Wisconsin. These seizures were possible because of international law enforcement and private sector coordination involving the partners listed below.

> To determine if you have been victimized, visit: haveibeenpwned.com or politie.nl/checkyourhack

Been active on Genesis Market? In contact with Genesis Market administrators? Email us, we're interested: FBIMW-Genesis@fbi.gov

SEUR POL

EUROJUST

nal Crime Aner

Federal Criminal Police Office

Disruption

POLIT

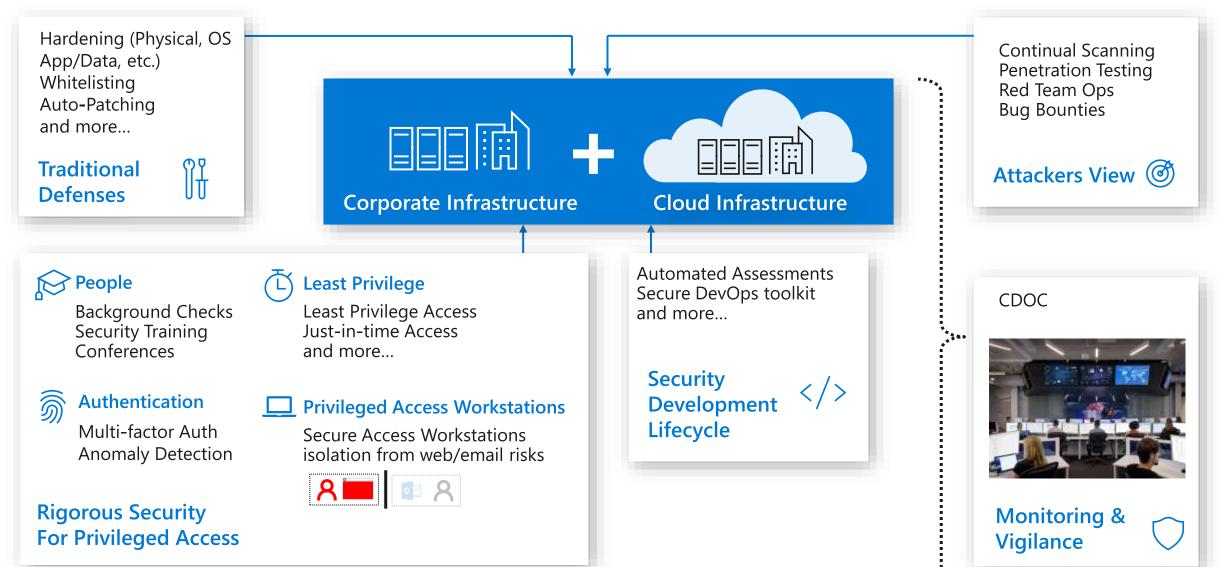
Defence: Are we talking about security of the cloud...

Source: https://www.publicdomainpictures.net/en/view-image.php?image=338689 (Creative Commons)

...or security *in* the cloud?

Source: https://www.publicdomainpictures.net/en/view-image.php?image=338689 (Creative Commons)

Defence: Microsoft protecting Microsoft



But it's a shared responsibility

NOT RESPONSIBLE FOR ACCIDENTS

Source: https://flic.kr/p/5hdXSR (Creative Commons)

One cloud is not like the other

The (almost) 10 laws of Cybersecurity Risk

LAW

173

ORTS

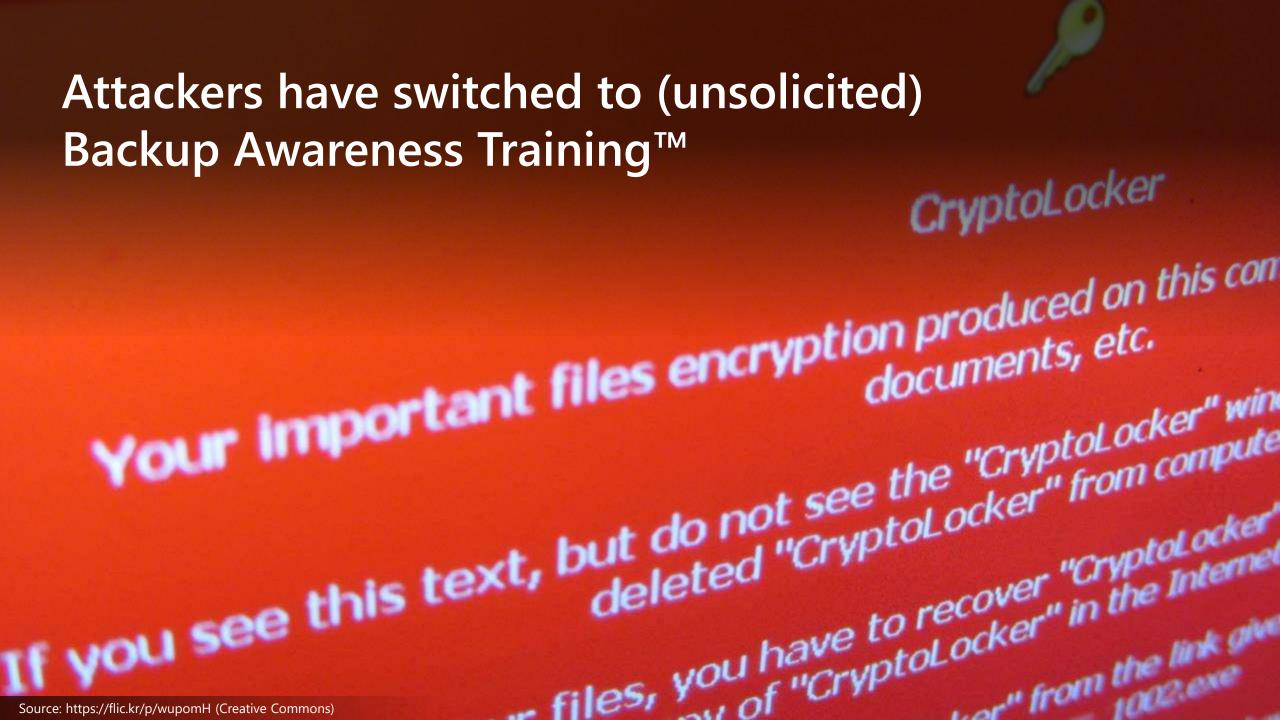
EPORTS

179.04 5

Source: https://learn.microsoft.com/en-gb/security/compass/ten-laws-of-security

#1 Security success is ruining the attacker's Return on Investment

The Business Model Canvas			Designed for:	Designed by:	Date: Version:
Key Partners	Ø	Key Activities	Value Propositions	Customer Relationships 🖤	Customer Segments
		Key Resources	1	Channels 💭	
Source: Strategyzer					



Fundamental hygiene matters

98%

Basic security hygiene still protects against 98% of attacks

Key

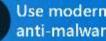
B)



Enable multifactor authentication



Apply Zero Trust principles



Use modern anti-malware



Protect data Ē₀

Source: Microsoft Digital Defense Report (https://aka.ms/MDDR)

#2 Not keeping up is falling behind





N





U.





So take the first leap to just get started...!

Source: https://flic.kr/p/PMW9fP (Creative Commons)

#3 Productivity always wins

Cast-

Source: https://flic.kr/p/bNU5cF (Creative Commons)

#3 Productivity always wins

KEEP OFF THE GRASS DOGS TOO

Source: https://flic.kr/p/6833R6 (Creative Commons)

#4 Attackers don't care



#5 Ruthless prioritisation is a survival skill

CHANGED

PRIORITIES

AHEAD

Source: https://flic.kr/p/7i4Xdw (Creative Commons)

Focus on what really causes harm

FARCE E

CCIDENT

Source: https://flic.kr/p/fk4Eyx (Creative Commons)

So: better *Buienradar* or just take your umbrella?

Source: https://www.publicdomainpictures.net/en/view-image.php?image=338689 (Creative Commons)

Security "the museum way"

Resilient: be able to respond and recover

RESCUE

Source: https://flic.kr/p/oREwdW - Creative Commons

#6 Cybersecurity is a team sport

21

Data sharing across our supply chain...

VENDOR RISK ASSESSMENT QUESTIONNAIRE TEMPLATE

	VENDOR TYPE	GOVERNING BODY	DATE OF LAST UPDATE	
ID No.	CATEGORY	QUESTION REFERENCE	ADDITIONAL INFORMATION	
1.0	Information Security			
1.1	Does your organization maintain a security program?			
1.2	Who is responsible for managing the security program?			
1.3	Does your organization have a public information security policy?		Request a link to policy	
1.4	What guidelines does your security program follow?			
2.0	Data Center Security			
2.1	Do you work in a shared office space?			
2.2	Is there a protocol in place for operations when your office is inaccessible?			
2.3	Is there a policy in place for physical security requirements for your business?			
2.4	What are the geographic locations of your data centers?			
3.0	Web Application Security			
3.1	What is the name of your web application? What is its function?			
3.2	How do you report application security vulnerabilities?			
3.3	Does your web application have an SSL certificate?			
3.4	Does your application offer single sign-on (SSO)?			
4.0	Infrastructure Protection			
4.1	Do you use a VPN?	National Institute of Standards and Technology (NIST)		
ource: a th	ird party risk template near you			

Are we partner or supplier?

Scale matters

..

--

--

....

56

...

...

-

-

-

-

-

11

...

...

..

--

...

--

1400

1916

7974

. .

. .

. .

...

..

2.0

#7 Your network isn't as trustworthy as you think it is

Source: https://flic.kr/p/7KY3mj (Creative Commons)

Zero trust: Assume breach

Zero trust: Assume breach & minimise impact

Zero trust: Verify explicitly

Source: https://twitter.com/Efteling/status/1035135919358181376/photo/1

Zero trust: Use least privileged access

Source: https://flic.kr/p/5zPpQL (Creative Commons)

#10 (yes, we skipped 8 and 9) Technology doesn't solve people and process problems

Source: https://unsplash.com/photos/4lxPVkFGJGI



Announcing

Microsoft Security Copilot

Source: https://www.microsoft.com/en-us/security/business/ai-machine-learning/microsoft-security-copilot#demo

Source: https://flic.kr/p/6WAFYy (Creative Commons)

#11 (bonus) Let security be the keel to control drift

NUSTR

Which questions can I answer for you?

How can we get our organisations on their bikes?

EXPLORE

Source: https://flic.kr/p/6opsy3 (Creative Commons

Thank you!

Jelle Niemantsverdriet



jelle.niemantsverdriet@microsoft.com @jelle_n linkedin.com/in/jelleniemantsverdriet/ EXPLORE

Source: https://flic.kr/p/6opsy3 (Creative Commons