

A red-tinted background featuring a globe with a network of white lines and dots, suggesting a global network or data flow.

Die dunkle Seite des Web

Trickbetrug und Datendiebstahl

Michael Haas

Area Sales Director Central Europe

michael.haas@watchguard.com

Agenda

- 1. What Is the Dark Web**
- 2. How Cyber Criminals Get Your Data**
- 3. Defending Your Data**



What Is the Dark Web

First... What Is the Surface Web?



The **Surface Web** is anything that can be indexed by a search engine

- Search engines crawl web pages
- Crawler follows links to other pages
- Crawled links are indexed

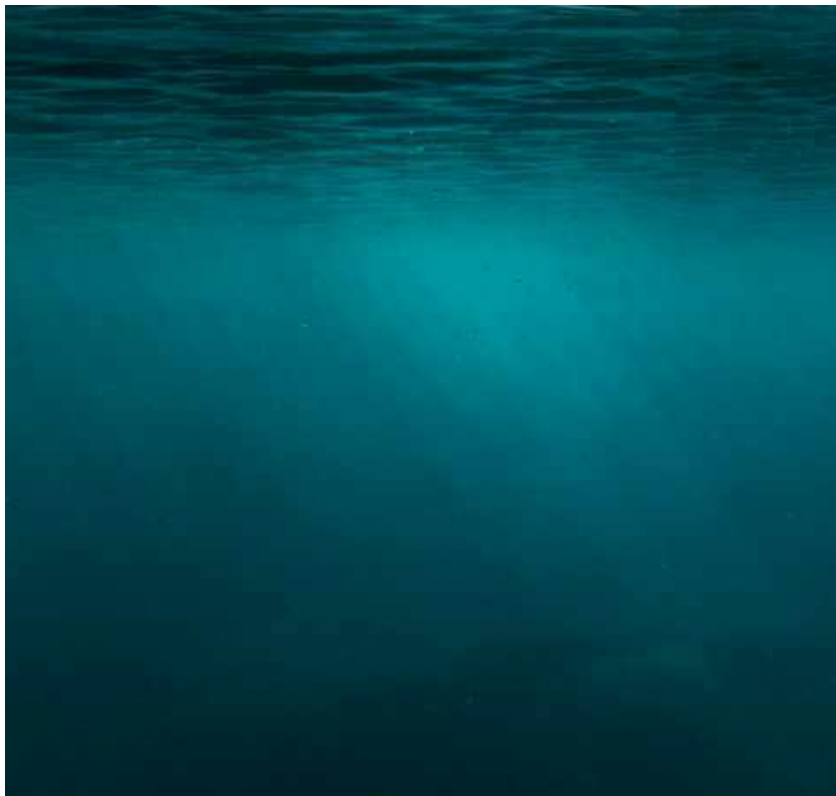
What Is the Deep Web?



The **Deep Web** is anything that search engine crawlers can't find

- Pages hidden behind search filters
- Un-linked pages
- Pages gated behind authentication

What Is the Dark Web?



The **Dark Web** is a portion of the Deep Web that is intentionally hidden and inaccessible through normal web browsers

- Requires special software to access
- TOR – The Onion Router
- I2P – Invisible Internet Project

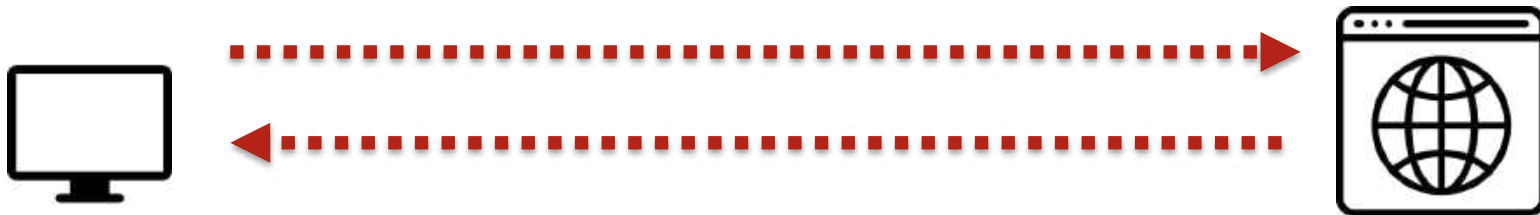
Asymmetric Cryptography 101

Asymmetric cryptography uses **two different keys** for encrypting and decrypting data.



- Public key & private key
- Data encrypted with one key can only be decrypted using the other key

How Does TOR Work?



http://

IP

[Data]

IP

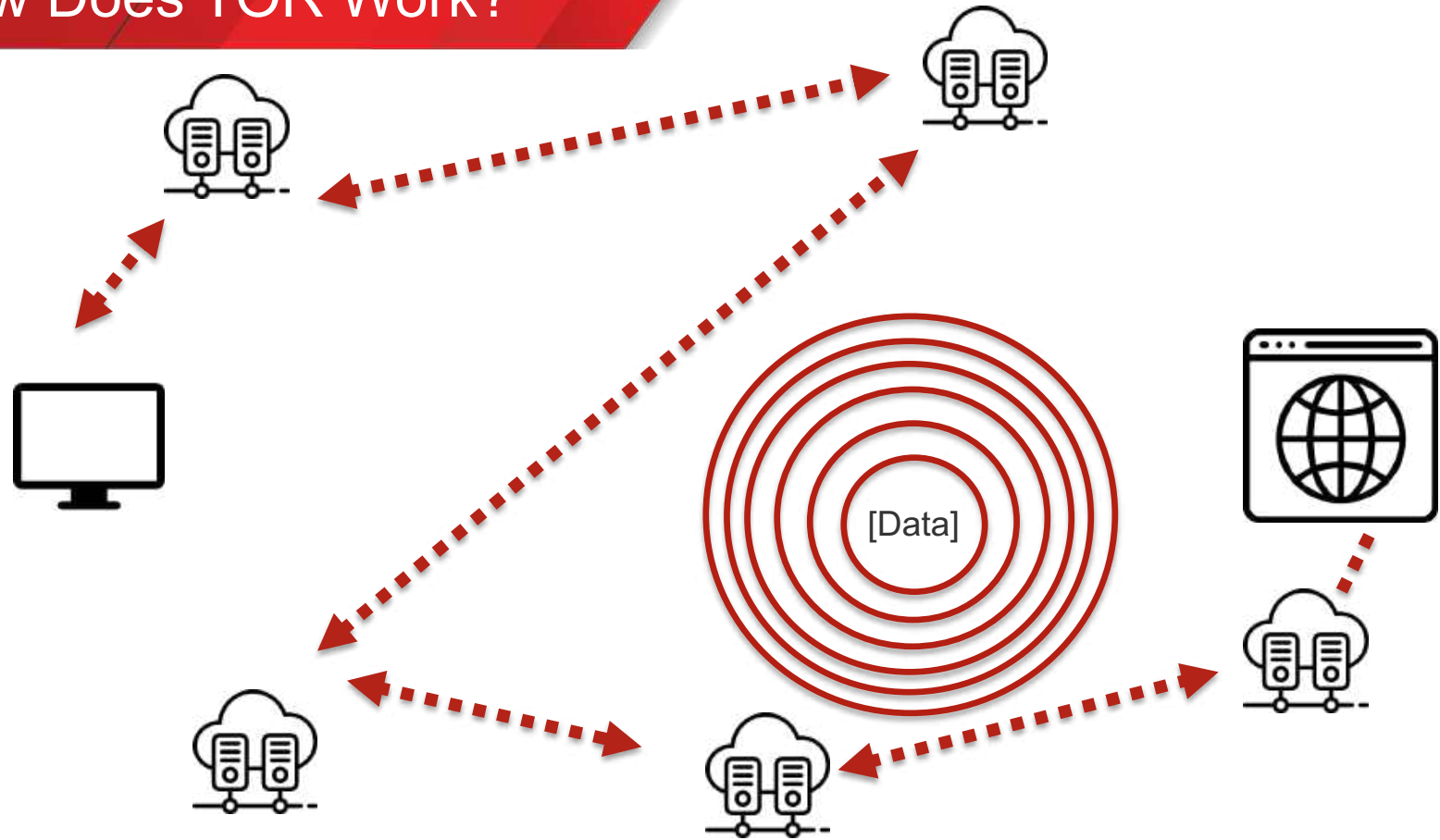
https://

IP

X98%u02r zr234%\$#6594

IP

How Does TOR Work?



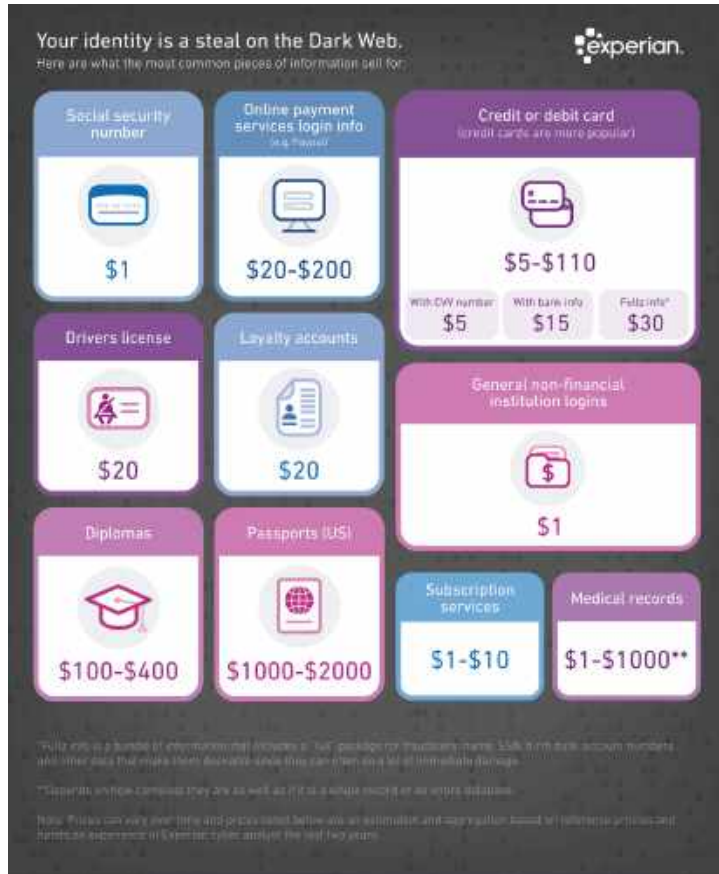
Where Did TOR Come From?

- Onion Routing was developed by U.S. Naval Research Laboratory employees and several computer scientists
 - Further developed by DARPA
- Designed to protect U.S. intelligence communications
- Maintained by The Tor Project
 - Initially sponsored by the Electronic Frontier Foundation (EFF)
 - Majority of funding still comes from the U.S. government

What Sites Are on the Dark Web?

- Facebook: facebookcorewwi.onion
 - Yes... Even the dark web can't escape
- The Hidden Wiki: zqktlwi4fecvo6ri.onion
 - List of all “public” dark web sites
- Marketplaces for anything and everything
 - Quite literally anything

Data on the Dark Web



- PII
 - Social security numbers
 - Medical records

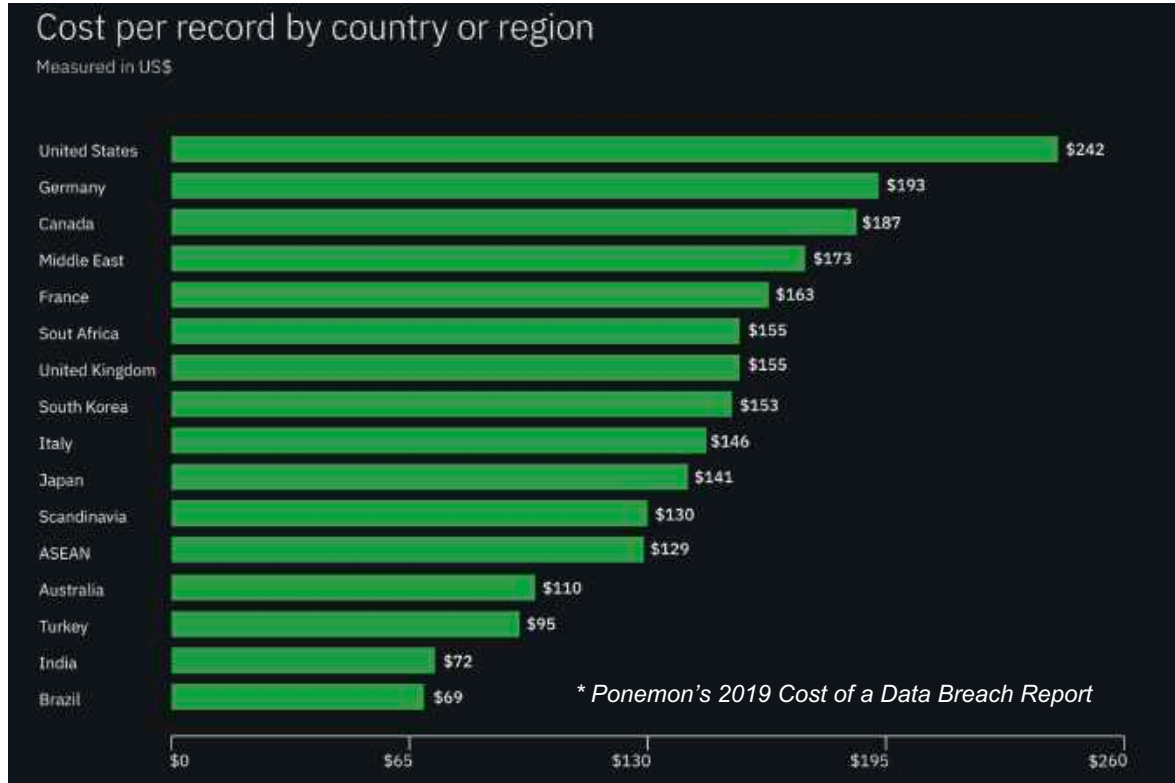
- Password dumps

- Intellectual property

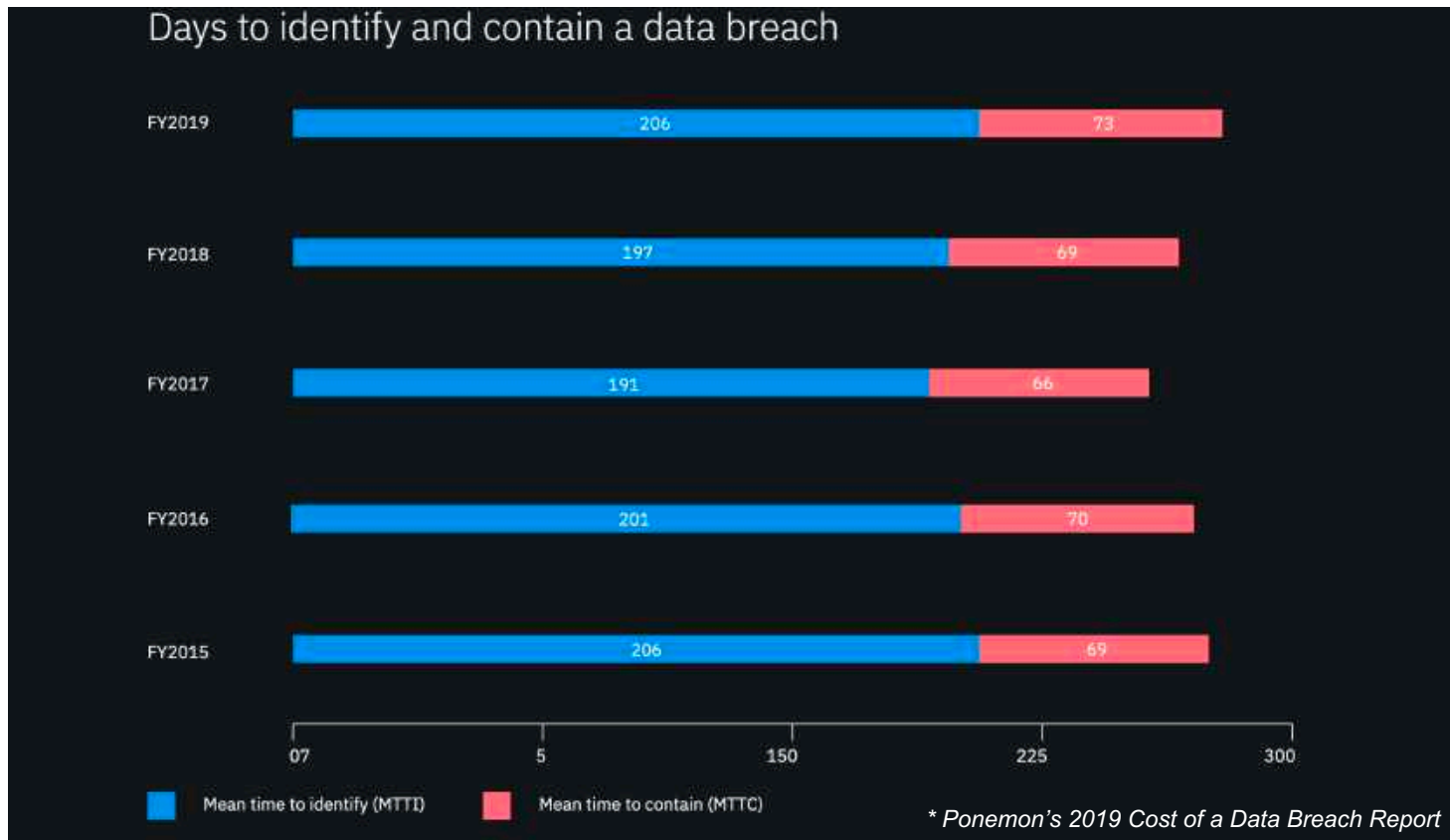


Breaches By The Numbers

Breach Costs Rise Slightly



Companies Are Still Too Slow at Detecting Breaches



Stolen

Data Breach Investigations Report 2020 von Verizon Business **Geld hält die Welt der Cyber-Kriminalität am Laufen**

27.05.20 | Redakteur: Peter Schmitz

- Use of s
- Use of b
- Exploit v
- Brute fo
- Buffer o
- Abuse o
- RFI
- SQLI
- Other
- 0%
- Breach

Der neue „Verizon Business 2020 Data Breach Investigations Report“ (DBIR 2020) zeigt, dass finanzieller Nutzen weiterhin der wesentliche Treiber für Cyber-Kriminalität ist: Fast neun von zehn (86 Prozent) der untersuchten Kompromittierungen sind finanziell motiviert, die Mehrheit (70 Prozent) wird weiter von externen Akteuren verursacht, 55 Prozent davon durch das organisierte Verbrechen.

Der „Verizon Business 2020 Data Breach Investigations Report“ (DBIR 2020) berichtet über einen Anstieg der Kompromittierungen von Webanwendungen um das Zweifache auf 43 Prozent im Jahresvergleich. **In über 80 Prozent dieser Fälle wurden gestohlene Zugangsdaten verwendet** – ein beunruhigender Trend, da geschäftskritische Workflows immer mehr in die Cloud verlagert werden. Auch bei Ransomware war ein leichter Anstieg zu verzeichnen, der bei 27 Prozent der Malware-Vorfälle festgestellt wurde (im Vergleich zu 24 Prozent im DBIR 2019). 18 Prozent der Organisationen gaben an, im vergangenen Jahr mindestens einen Ransomware-Angriff blockiert zu haben.

available
 e dark
 s lead



How Do They Get Your Data?

Spear Phishing

A very well designed and targeted email masquerading as legitimate correspondence. It tries to socially engineer you into doing something you shouldn't.



Quick History

- Phishing around since the 90s
- Notable *spear* phishing started 2010
- RSA's hack started w/spear phishing (2011)
- Anthem breach was a spear phish (2015)
- DNC Hack (2016), etc...



Latest Evolutions

- Automated social network recon
- Org partner mapping
- Brand impersonation
- Whaling & targeted smishing/vishing




Targets, Tactics, and Trends

- 90-95% of breaches start with spear phish
- 94% of spear phish use files not links
- Leading cause of account takeover
- 28% of phishing is targeted
- 30% open spear phish; ~14% click
- Lowest volume, but highest impact cost



← → ↻ <https://servicemanager00.blab.core.windows.net/5eb/currentusers.html?api=rbcat=2019-02-28T12:42:41Z&se=2019-04-28T19:42:41Z&spr=https&wy=2018-03-26&sig=Ls4wdGcE4rIbF78uEVhIGcbAE3P0H5i2Bd1Mvo4QyF94dw%3D&sr=href> ☆


App




The image shows a Microsoft account selection dialog box overlaid on a blurred background of a city at sunset. The dialog box has the Microsoft logo at the top left. Below the logo, it says "Pick an account". There are two options: a profile icon with the email address "sam@samscompany123.com" and a plus sign icon with the text "Use another account".

Microsoft

Pick an account

 sam@samscompany123.com

 Use another account

©2019 [Terms of use](#) [Privacy & cookies](#)

Account Takeover

An attack where the invader successfully logs into an org impersonating a trusted employee. Often involves lost or stolen credentials.



Quick History

- 2002: First mandatory breach disclosure law
- 2004: Gates, "passwords are dead"
- 2011: Sony PSN lost 77m passwords
- 2013: Google exec, "passwords are dead"
- 2013 Yahoo lost 1b passwords
- 2019: Collection 1-5 leak, 22b passwords



Latest Evolutions

- Password Spraying (common passwords)
- Credential Stuffing (leaked passwords)
- Mimikatz & WCE
- SMS 2FA bypass
- SIM swapping



Targets, Tactics, and Trends

- Reddit (2FA bypass)
- Cred Stuffing:
 - Citrix
 - HSBC
 - State Farm
 - Retail vertical
- Passwords still top factor in 2020



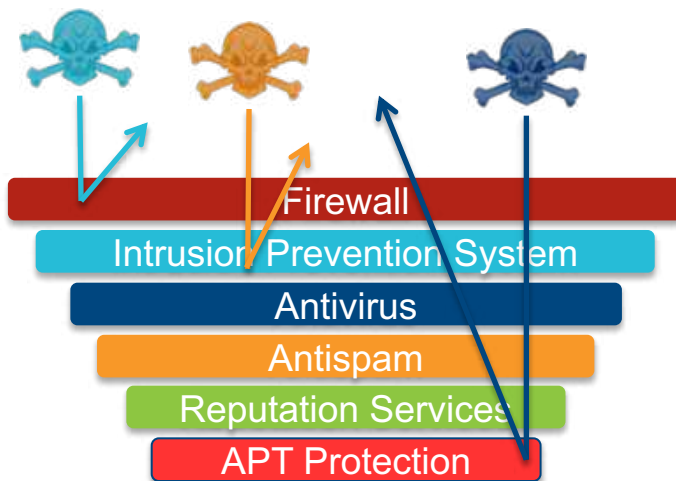


Defending Your Data

Prevention: Defense In Depth

Advanced threats, by definition, leverage **multiple vectors of attack.**

No single defense will protect you completely from computer attacks...



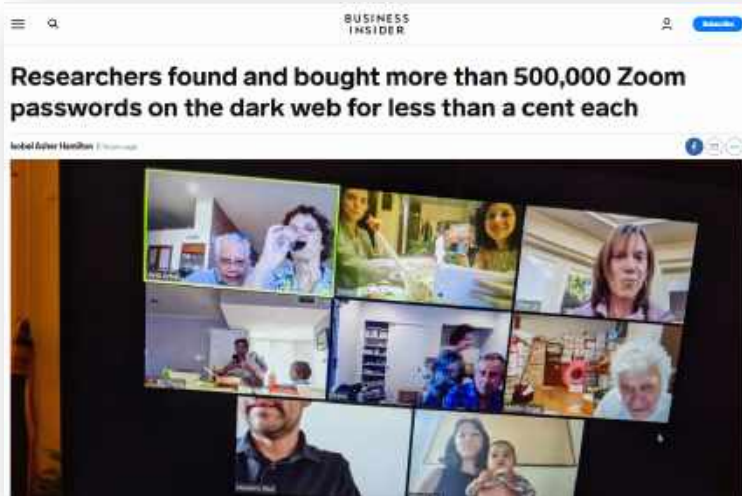
The **more layers of security** you have, the **higher chance** an additional layer catches an advanced threat other layers miss.

Phishing and Account Takeover Defense

- Multi-Factor Authentication
- Phishing Awareness Training
- DNS Firewalling
- Advanced Malware Protection



Are You Still Using Stolen Credentials?



- “Credential stuffing” was used to breach more than 500k accounts
- Users are using same passwords from previous breaches

5

Average number of passwords a users **will try to use on most accounts**, with small variations

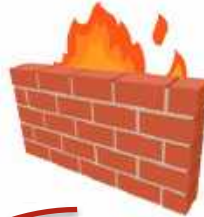


MFA Can Protect... and Block Attacks!



Dark Web Stolen Credential:

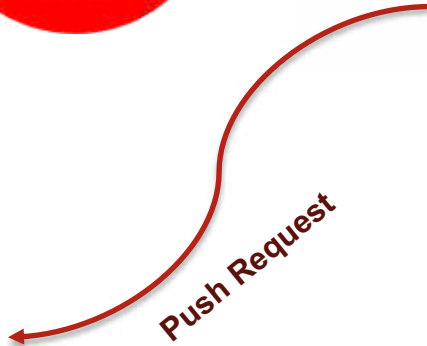
Username: mhaas
Password: Leo2012



My Network



Michael
Working from Home



#Sichersein

- Informieren Sie sich in Sozialen Netzen
- Treffpunkt #Sichersein: Die Security Morningshow
- #Sichersein in Kürze: 3 Fragen an...



Danke
Bleiben Sie gesund!

Michael Haas
michael.haas@watchguard.com
+49 170 7727415