

REMOTE ACCESS SECURITY IN THE AGE OF CORONA

Tuesday, June 9, 2020 | 2:00PM-3:00PM



1. CURRENT OPERATING ENVIRONMENT FOR COVID-19
2. TELEWORKING OPERATING CONCERNS
3. EMERGING RISKS
4. MANAGING RISKS & OPERATING CONCERNS



In the current business landscape companies are required to adapt new practices

- The number of employees working remotely has increased dramatically
 - Global Workplace Analytics estimates that work-at-home will save U.S. employers over \$30 Billion a day in what would have otherwise been lost productivity during office closures due to COVID-19

- Companies are providing teleworkers required access to services through remote connections into their infrastructure
 - Services form on premise resources (Internal Network, systems and applications)
 - Cloud services
 - Public internet
 - Collaboration services

Changing operations is a financial impact

Operating Concerns

- Cost of laptops for remote access
 - Alternative approach is that many companies are allowing employees to connect in using their home computer

- Infrastructure to support increased remote workers
 - Increased teleworker connections to requires additional resources, incurs greater costs, and decreases performance
 - Teleworkers require access to company network first establish a trusted connection through VPN
 - Aggregating all teleworker traffic through a single location to enforce security policy at a central location
 - This security pattern also enables teleworkers to leverage the same connectivity to internal and cloud services / applications

EMERGING RISKS

- State sponsored attacks on new targets
 - The usual actors: China, Iran, Russia and North Korea
 - New targets: Restaurants and Delivery
 - Scenario: Mimic or hack into new targets - Gain access online accounts (Google/Yahoo...) – Gain access to Government and Healthcare worker work account

- Increased PHISHING attacks
 - PC Magazine - Phishing Attacks Increase 350 Percent Amid COVID-19 Quarantine
 - Zscaler - 20,000 unique incidents of phishing attacks

- Increased attacks on remote workers
 - CNET - 7,000 incidents in which victims were tricked into starting a download of malware, all of which referenced the health crisis.

MANAGING RISKS & OPERATING CONCERNS

- **Laptops, home computer, PHISHING and attacks on remote workers**
 - Multifactor authentications (MFA) must be deployed for all users especially staff connecting via home computer
 - MFA for privileged accounts and staff with access to sensitive an private information
 - Standard security build and security tools that cannot be turned off
- **Infrastructure to support increased remote workers**
 - Segmentation of environment reduce overall impact and increase security
 - Teleworkers connect directly to the cloud for services where the same security policy can be enforces
- **State sponsored attacks on new targets**
 - Ensure passwords are complex and require regular changing of passwords
 - Reinforce to not use same passwords as personnel passwords and provide guidance for all employees to change password
 - Block all access outside the GEO location of workforce via web browser and conditional access rules in the cloud

Have employees check there work and personal accounts for confirmed data exfiltration at: <https://haveibeenpwned.com/>

The screenshot shows the 1Password website interface. At the top, it says "Oh no — pwned!" and "Pwned on 3 breached sites and found no pastes (subscribe to search sensitive breaches)". Below this is a section titled "3 Steps to better security" with a "Start using 1Password.com" button. The steps are: Step 1: Protect yourself using 1Password to generate and save strong passwords for each website. Step 2: Enable 2 factor authentication and store the codes inside your 1Password account. Step 3: Subscribe to notifications for any other breaches. Then just change that unique password. Below the steps is a "Why 1Password?" section with social media icons and a "Donate" button. The bottom section is titled "Breaches you were pwned in" and lists three breaches: Houzz, MyFitnessPal, and MyHeritage, each with a brief description of the breach and the compromised data.

Oh no — pwned!
Pwned on 3 breached sites and found no pastes (subscribe to search sensitive breaches)

3 Steps to better security [Start using 1Password.com](#)

Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.

Step 2 Enable 2 factor authentication and store the codes inside your 1Password account.

Step 3 [Subscribe](#) to notifications for any other breaches. Then just change that unique password.

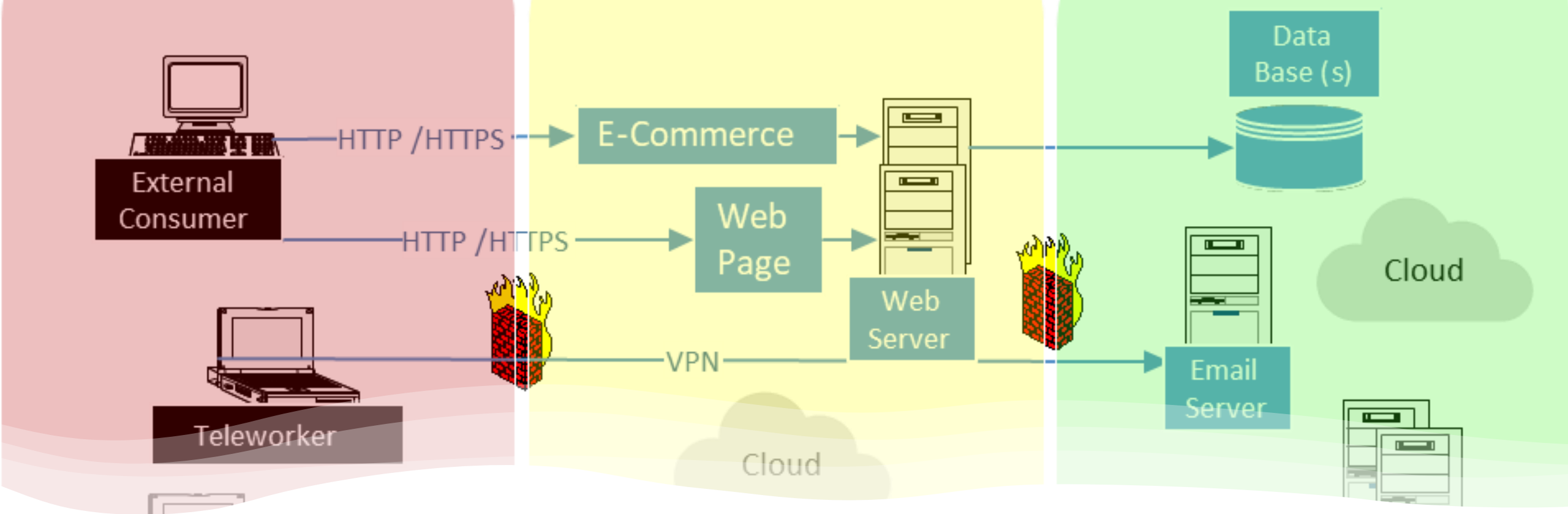
Why 1Password?
Donate

Breaches you were pwned in
A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

houzz Houzz: In mid 2018, the housing design website Houzz suffered a data breach. The company learned of the incident later that year then disclosed it to impacted members in February 2019. Almost 49 million unique email addresses were in the breach alongside names, IP addresses, geographic locations and either salted hashes of passwords or links to social media profiles used to authenticate to the service. The data was provided to HIBP by [dehashed.com](#).
Compromised data: Email addresses, Geographic locations, IP addresses, Names, Passwords, Social media profiles, Usernames

MyFitnessPal In February 2018, the diet and exercise service MyFitnessPal suffered a data breach. The incident exposed 144 million unique email addresses alongside usernames, IP addresses and passwords stored as SHA-1 and bcrypt hashes (the former for earlier accounts, the latter for newer accounts). In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it to be attributed to "BenjaminBlue@exploit.im".
Compromised data: Email addresses, IP addresses, Passwords, Usernames

MyHeritage In October 2017, the genealogy website MyHeritage suffered a data breach. The incident was reported 7 months later after a security researcher discovered the data and contacted MyHeritage. In total, more than 92M customer records were exposed and included email addresses and salted SHA-1 password hashes. In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it be attributed to "BenjaminBlue@exploit.im".
Compromised data: Email addresses, Passwords



***TELEWORKING PRE-COVID-19, 3.6% ESTIMATES RISE TO 25%-30% POST-COVID-19** * GLOBAL WORKPLACE ANALYTICS

- Zero Trust Architecture
 - Access based on user location, IP address and MFA, machine location and other data
 - Segmented networks based on purpose, sensitivity and criticality
 - Enforce common security policy on premise and in the cloud

PHILIP A. JONES

DIRECTOR - CYBERSECURITY

Telephone +1 813 760 5347

Philip.Jones@mazarsusa.com

My profile on [LinkedIn](#)



QUESTIONS AND ANSWERS

To ask questions, please use the **Q&A** box on the right-hand side of your screen

