TECHNICAL CHECKLIST

COVID-19: Thwarting Opportunistic Attackers

Fortify Security Defenses and Improve Situational Awareness

While the ramifications of the coronavirus global pandemic continue to worsen, opportunistic attackers are coming out in droves. From phishing campaigns to ransomware and malicious domains, attackers are seizing the opportunity to capitalize on this life changing crisis.

Proactively taking the needed steps to protect your work from home (WFH) and enterprise environments is critical to minimize risk. The first area of focus in both environments is to evaluate your attack surface. WFH certainly has a large impact here so it is important to reduce exposure and minimize the endpoints in your environment wherever possible.

Focusing on mobile device security, social activities, network monitoring and multifactor authentication will enable security teams to react quickly. The technical checklist that follows breaks down the steps you can take within each of these areas to harden security and expediate response times.

IMMEDIATE ACTIONABLE STEPS TO TAKE

Protect the WFH Environment

☐ **Attack surface management**
Continue to reduce the attack surface area of both corporate and BYOD assets and network connections

- Wireless networks, regardless of the hosts connecting, should be secured with proper encryption: Use WPA2 or WPA3 with a strong passphrase of at least 12 characters, or longer, comprised of complex characters
- Ensure that firmware is at the latest version for home routers/wireless access points, as well as other devices on the home network, such as network printers; If available, enable automatic updates
- Change default passwords on home routers/access points as well as other networked devices on the home network
- Ensure that when a wired connection is used, wireless access is turned off (this prevents potential bridging of networks)
- Ensure a minimum baseline standard is enforced against antivirus/anti-malware, operating systems type, version, and patch level and that web browsers are up to date; Meaning, antivirus/anti-malware subscriptions must be current, and the latest update should have occurred within a tolerable limit (usually 24 hours); Operating systems and browsers should have the latest security patches installed

☐ Attack surface management (continued)

- Ensure HTTPS is used wherever possible. Manually search or navigate to sensitive sites such as single-sign-on ("SSO") portals and financial sites

☐ **Mobile device security**

- On mobile devices, do not install mobile applications from untrusted (non-App store) or unauthorized repositories
- Ensure the wireless networks mobile devices connect to do not require new profiles to be installed

☐ **Social activities**

- Be wary of phone calls from unverified sources. If suspicious, hang up and verify from a trusted source
- Flag emails that contain a call to action, or subject lines relating to COVID-19/Coronavirus, economic stimulus claims or other economic relief
- Hover the mouse cursor over email links before clicking. Attackers can make a link appear legitimate but redirect to a hidden URL (see example below)

Protect the Enterprise

☐ Attack surface management

- Continue to reduce the attack surface area in the enterprise
- Deploy secured VPN, SSO and MDM. Offensively test all controls in these deployments to ensure efficacy of controls
- Configure full-tunneling VPN solutions if bandwidth is not an issue
- Allow split-tunneling for VPN connections in conjunction with a robust least-privilege policy for VPN traffic if bandwidth is a concern

☐ Network monitoring

- Increase network monitoring and logging around WFH users accessing trusted internal networks
- Consider implementing network EDR, lateral movement detection mechanisms, and/or deception technology in the networks where remote access solutions terminate to detect malicious traffic hiding amongst legitimate traffic
- Consider implementing full packet capture technologies to enhance logging, as well as for forensic purposes if a compromise occurs

Implement full packet capture for forensic purposes if a compromise occurs

☐ Consider also implementing deception technology on those same networks mobile device management (MDM)

- Ensure mobile device enrollment is authorized correctly to reduce an opportunistic attacker from registering an unauthorized device
- Align device enrollment authorization with the proper internal user identity and a corporate email. Consider using out-of-band authentication (OTP through SMS) for enrollment of the intended device
- Consider BYOD containers in the MDM solution, as well as application reputation and mobile anti-malware solutions as part of the MDM deployment

☐ Multifactor authentication

- Implement proper MFA controls for remote access solutions, including VPN, VDI and applications through SSO
- Follow best practice guidance from the solutions providers in deployment and configuration, as well as standards bodies around MFA
- Ensure that an OATH compliant MFA client is used where possible, and if MFA push is enabled, ensure users are educated around the solution. MFA push "fatigue" can be taken advantage of if credentials are compromised and users want to dismiss push notifications

In times of need or crisis, it can be challenging to know who to turn to for help and support. Optiv is here to provide our valued clients with the expertise, staffing and technology needed to ensure business continuity.

Please contact your Optiv sales representatives, as needed, during this tumultuous time.

Find Out More

Optiv Global Headquarters
1144 15th Street
Suite 2900
Denver, Colorado 80202
800.574.0896
optiv.com

Secure your security.™

Optiv is a security solutions integrator – a "one-stop" trusted partner with a singular focus on cybersecurity. Our end-to-end cybersecurity capabilities span risk management and transformation, cyber digital transformation, threat management, security operations, identity and data management, and integration and innovation, helping organizations realize stronger, simpler and more cost-efficient cybersecurity programs that support business requirements and outcomes. At Optiv, we are leading a completely new approach to cybersecurity that enables clients to innovate their consumption models, integrate infrastructure and technology to maximize value, achieve measurable outcomes, and realize complete solutions and business alignment. For more information about Optiv, please visit us at www.optiv.com.