Consider These **10 Critical Steps** to Prevent and Detect Ransomware Threats

Ransomware attacks are a serious global issue and getting worse – in fact, they are often considered the top cyber threat facing businesses today.[1] Ransomware statistics are staggering:

- **Damages to businesses and organizations are expected to be $20 billion in 2021[2]**
- **Global ransomware reports are up more than 715% from 2019 to 2020[3]**
- **Ransomware payments have increased 60% in value since 2019[4]**

Ransomware is a crisis that will only get worse as threat actors continue to grow in sophistication and expertise. Ransomware attackers often operate with the discipline and approach of a legitimate traditional business, except with criminal intent. Fortunately, there are strategies companies can take to reduce the risk of falling victim to a ransomware attack.

Consider these ten technologies and processes to help prevent and detect a ransomware attack. Each of these steps aligns closely with how attackers create and consummate their criminal activity. While some are costly, proactively implementing these steps now can mitigate the costs of business interruption, reputational damage, incident response and/or a ransomware payment.

1. **Phishing Awareness Training**, to educate employees and end-users on how to spot phishing emails and know the red flags to drive down clicks on the malicious emails many ransomware attackers use to gain a foothold in a network.

2. **Disabling Accessibility of Remote Desktop Directly from the Internet**, to prevent ransomware attackers from brute-forcing Internet-facing RDP services to gain entry into a network.

3. **Properly Configured URL Filtering and E-mail Attachment Sandboxing**, to prevent malware contained in ransomware emails from executing or going unnoticed.

4. **An Advanced Endpoint Detection and Response ("EDR") Solution**, to detect and potentially quarantine ransomware and other advanced malware, and also to facilitate enterprise forensics in the event of an attack.

5. **An Advanced Malware Detection Tool that Inspects Network Traffic**, to identify ransomware and other malicious packets or network traffic flowing over the wire.

6. **16+ Character Service Account and Domain Admin Passwords**, to prevent ransomware and other hackers from cracking weak admin user names and passwords. Optimally, these strong passwords should be rotated regularly, using a Privileged Access Management (PAM) tool. Ransomware attackers use these cracked credentials to move laterally and deploy their ransomware.

7. **Lateral Movement Detection Tools.** After gaining a foothold, ransomware actors typically move laterally using compromised IT credentials. Detecting that anomalous lateral movement normally enables the attack be shut down before ransomware is deployed.

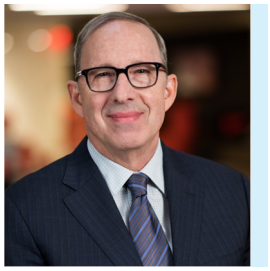
8. **A Properly Configured Security Information and Event Management ("SIEM") Platform** that aggregates event, security, firewall and other logs. Trying to respond to and recover from a ransomware attack without a SIEM is very difficult, as visibility through local, non-centralized logs is often poor.

9. **A Continuous Security Monitoring Function**, which provides continuous monitoring and threat hunting using collected logs and alerts.

10. **Locking Down Software Deployment and Remote Access Tools** (such as SCCM, PDQ, and PsExec) to a small set of privileged accounts with multi-factor authentication where possible. Once they have secured elevated privileges, ransomware attackers typically commandeer SCCM/PDQ/PsExec accounts to push the ransomware executable across the network.

Learn more about how Aon's cyber security solutions can help your business by visiting **aon.com/cyber-solutions**

AON
Empower Results®



About the Author

Eric M. Friedberg

Co-President Stroz Friedberg, an Aon Company

Eric M. Friedberg is co-founder and Co-President of Stroz Friedberg, LLC, a cyber consultancy and technical services firm acquired by Aon plc in 2016. Mr. Friedberg has 30 years of public and private sector experience in law, cyber-crime response, cyber-governance, IT security, forensics, investigations and e-discovery. His expertise is sought by boards, audit committees, C-suites, law firms and the courts.

Cyber Solutions Contacts

Eric Friedberg
Co-President Stroz Friedberg, an Aon Company
+1 212.981.6536
eric.friedberg@aon.com

AMERICAS

Christian E. Hoffman
CEO, Cyber Solutions North America
+1 212.441.2263
christian.hoffman@aon.com

Beatrice Conner
Managing Director, Advisory Services
+1 214.377.4567
beatrice.conner@aon.com

Chad Pinson
DFIR, Investigations, & Engagement Management
+1 214.377.4553
chad.pinson@aon.com

Brent Rieth
U.S. Practice Leader, E&O/ Cyber Broking
+ 1 312.381.3141
brent.rieth@aon.com

Ady Sharma
Vice President, Canada Cyber Sales Operations
+1 416.263.7876
ady.sharma@aon.ca

Katharine Hall
Senior Vice President, Canada Cyber Practice Leader
+1 780.423.9820
katharine.hall@aon.ca

LATAM

Temo Garcia
Senior Broker & U.S./ Latin America Cyber Champion
+1 312.381.4398
temo.garcia@aon.com

EMEA

Onno Janssen
CEO, EMEA
+49 (4) 03.605.3608
onno.janssen@aon.com

Richard Hanlon
Chief Commercial Officer
+353 1 266.6443
richard.hanlon@aon.ie

APAC

Michael Parrant
Cyber Insurance Practice Leader
+6 (141) 333.9783
michael.j.parrant@aon.com

Andrew Mahony
Regional Director
+6 (58) 428.1965
andrew.mahony@aon.com

Chris McLaughlin
Director
+61 29253.7792
chris.mclaughlin@aon.com

Sources

1. **https://www.inc.com/adam-levin/ransomware-is-number-one-cyber-threat-this-year-heres-what-you-can-do.html**
2. **"2019 Cybersecurity Almanac," Cisco and Cybersecurity Ventures, 2019**
3. **Bitdefender's Mid-Year Threat Landscape Report 2020, page 14**
4. **Coveware Ransomware Marketplace Report, August 3, 2020**

About Cyber Solutions: Aon's Cyber Solutions offers holistic cyber risk management, unsurpassed investigative skills, and proprietary technologies to help clients uncover and quantify cyber risks, protect critical assets, and recover from cyber incidents.

About Aon: Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

Empower Results®