
FOSTER
INSTITUTE
Please Do Not Distribute.
These Slides are for Member
Participants and Their
Companies ONLY
© The Foster Institute, Inc.
mike@fosterinstitute.com

1


Opportunities to Plant Back Doors
• SolarWinds Breach
– Discovered 12/8/2020 (1/2019)
• Apache Log4j RCE
– Discovered12/10/2021 (7/2014)
• Microsoft Exchange and RDP Exploits
– Ongoing with companies not upgraded and protected

2


You Must Protect
• Your Websites / Web Applications
• Your Network
• Cloud Services You Use
• You Personally as a High Net Worth Individual

3

Geo-Block All Non-Essential Countries

- Limit Access to Your Web Applications by Country
- Network Firewall: Traffic's Source and Destination
- Office 365 Conditional Access by Country
- Email Messages - Spam Filter Geo Filtering

4

Web Content Filtering for if a User "Clicks"

- You Might be Surprised what Countries Your Sites Access
- Be Careful Not To Overwhelm Your IT Pros
- Different Tactic:
  - With other recommendations, block all and allow specific countries
  - For web content filtering, consider blocking specific countries

5

Always use 2-Step Login For:

- SaaS Cloud Software
- VPN Connections
- Remote Desktop Connections

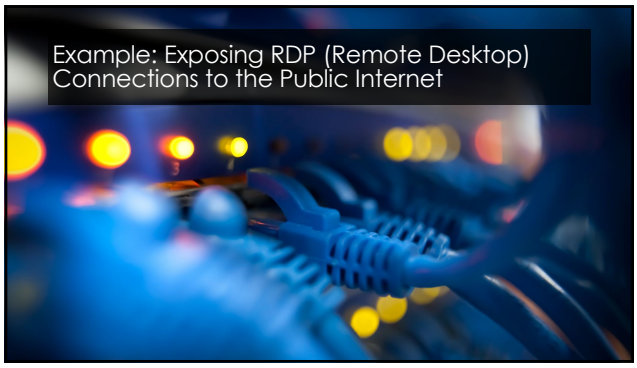
6

Firewalls

- Close all Ports
- Expose Nothing (except what is essential)
- Limit Exposure to Specific Addresses

7

Example: Exposing RDP (Remote Desktop) Connections to the Public Internet



8

Attackers Break Features

- Never Trust Any Features to Protect You
- Do not trust the firewall works flawlessly
- Testing is Essential

9

Put Your Email Servers into Action!

- Block fraudulent messages from reaching users' inboxes
- Protects Your reputation from your customers receiving fraudulent messages from you
- SPF, DKIM, and DMARC

10

The Essential Basics

- Critical Updates and Security Patches
- No "Local Admin" users
- Anti-Virus or Endpoint Detection and Response tools
- Application Control

11