Critical Hygiene for Preventing Major Breaches

Jonathan Trull
Microsoft Enterprise Cybersecurity Group
@jonathanantrull

Tony Sager
Center for Internet Security
@CISecurity

Mark Simos
Microsoft Enterprise Cybersecurity Group
@MarkSimos
The CISO Challenge

Quote from unnamed CFO:

“The problem with CISOs, and the entire cyber security field for that matter, is that you keep asking for more money and resources but can’t guarantee or even articulate what I’m buying.”
<table>
<thead>
<tr>
<th>Complexity</th>
<th>Velocity</th>
<th>Volume</th>
</tr>
</thead>
<tbody>
<tr>
<td>23% of recipients opened phishing messages</td>
<td>50% of those who open and click attachments do so within the first hour</td>
<td>6,449 new vulnerabilities in 2016</td>
</tr>
<tr>
<td></td>
<td>24 hours from click to domain compromise</td>
<td>16% of new vulnerabilities rated as critical</td>
</tr>
<tr>
<td></td>
<td></td>
<td>100Ks of detections per day</td>
</tr>
</tbody>
</table>

The Playing Field
Microsoft Threat Landscape – Last 6 Months

68 incidents across 8 different countries responded to by Global Incident Response & Recovery Team

15,000 cases worked by the Cyber Defense Operations Center

85 – 90% of Incidents could have been prevented by:

1. Patching Critical Vulnerabilities
2. Removing Administrative Privileges
3. Using Strong Passwords / MFA
CISO’s Coefficient

\[ \text{CISO’s Coefficient} = ((\text{Team Efficiency}) \times -\text{(Business Disruption)}) \]

(Return on Investment)
Key Objectives

1. Focus on controls that deliver highest ROI
2. Set and maintain foundation for long-term, sustainable program
3. Minimize controls that disrupt the business and maximize controls that increase security team’s effectiveness and efficiency
The “Fog of More”

- anti-malware
- governance
- continuous monitoring
- baseline configuration
- standards
- SDL
- audit logs
- risk management framework
- encryption
- threat intelligence
- user awareness training
- two-factor authentication
- security controls
- need-to-know
- supply-chain security
- DLP
- certification
- penetration testing
- threat feed
- best practice
- virtualization
- SIEM
- sandbox
- compliance
- security bulletins
- incident response
- browser isolation
- maturity model
- whitelisting
- audit logs
- baseline configuration
- standards
- SDL
- audit logs
- risk management framework
- encryption
- threat intelligence
- user awareness training
- two-factor authentication
- security controls
- need-to-know
- supply-chain security
- DLP
- certification
- penetration testing
- threat feed
- best practice
- virtualization
- SIEM
- sandbox
- compliance
- security bulletins
- incident response
- browser isolation
- maturity model
- whitelisting
The Defender’s Challenges

- **What’s** the right thing to do, and **how much** do I need to do?
- **How** do I actually do it?
- And then how do I demonstrate to **others** that I have done the right thing?
A few cybersecurity lessons

● Cybersecurity is like a movie
  ● “Groundhog Day”, not “Independence Day”

● Cyber Defense = Information Management
  ● not Information Sharing, not technology; the most important verb is translate
  ● How do I translate millions of data points into the most effective action, at the right time?

● Defenders have limits: info, choices, budget, time.

● Attackers don’t perform magic
  ● They have a plan, a budget, a Boss
# The CIS Community Attack Model

<table>
<thead>
<tr>
<th>Controls</th>
<th>Initial Recon</th>
<th>Acquire/Develop Tools</th>
<th>Delivery</th>
<th>Initial Compromise</th>
<th>Misuse/Escalate Privilege</th>
<th>In</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td>control of HW, SW inventory</td>
<td>threat intelligence</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protect</td>
<td>firewall; mail gateway filtering; web filtering; manage ports, protocols, services</td>
<td>threat intelligence; control of SW execution; app whitelisting</td>
<td>continuous vulnerability assessment; firewall; mail gateway filtering; web filtering; secure remote access</td>
<td>patching; hardened configurations; HIPS; anti-malware; containerization; app whitelisting; Data Execution Prevention</td>
<td>control of admin privilege; data security</td>
<td>control of admin segments</td>
</tr>
<tr>
<td>Detect</td>
<td>firewall; honeypot; NW authentication; NW logs</td>
<td>audit logs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Respond</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

[Image]
Calculating Security ROI

Defender Return:
- Ruin Attacker ROI
  - Deters opportunistic attacks
  - Slows or stops determined attacks

Attacker Return: Successful Attacks
- Difficult to influence attacker monetization of your data

Attacker Investment: Cost of Attack
- Prioritizing defenses can rapidly raise attacker costs

Defender Investment:
- Security Budget
- Team Time/Attention

Security Return on Investment (SROI)
Focus on Raising Attacker Cost

- Ruin Attacker’s Economic Model
- Break the Known Attack Playbook
- Rapid Response and Recovery
- Eliminate other attack vectors

Desired Outcome: Change the Defender’s Dilemma to an Attacker’s Dilemma
Methodology

FIRST 30 DAYS

Meaningful positive impact with near-zero friction
- Zero or minimal risk of operational downtime
- Requires no new skillsets
- Tooling must be set up quickly (e.g. existing web services / appliances in online marketplace, etc.)

FIRST 90 DAYS

A single investment provides to significant positive impact
- Learning and applying a new skillset (e.g. threat modelling, code review, manage new tool/capability)
- Perform Testing to Mitigate operational impact
- Changes with broad impact (change helpdesk support procedures, user experience, etc.)

NEXT QUARTER AND BEYOND

Build meaningful resilience to long term threats
- Lower organizational risk by sustaining initial investments and addressing foundational elements
Phase 1 Critical Mitigations: Typical Attack Chain
Compromises privileged access

1. Beachhead (Phishing Attack, etc.)
2. Lateral Movement
   a. Steal Credentials
   b. Compromise more hosts & credentials
3. Privilege Escalation
   a. Get Domain Admin credentials
4. Execute Attacker Mission
   a. Steal data, destroy systems, etc.
   b. Persist Presence

24-48 Hours
Credential Theft Demonstration

http://aka.ms/credtheftdemo
Protecting Active Directory and Admin privileges

1. Separate Admin account for admin tasks
2. Privileged Access Workstations (PAWs)
   Phase 1 - Active Directory admins
   http://Aka.ms/CyberPAW
3. Unique Local Admin Passwords for Workstations
   http://Aka.ms/LAPS
4. Unique Local Admin Passwords for Servers
   http://Aka.ms/LAPS

First response to the most frequently used attack techniques
Protecting Active Directory and Admin privileges

1. Privileged Access Workstations (PAWs)  
   Phases 2 and 3 –All Admins and additional hardening (Credential Guard, RDP Restricted Admin, etc.)  
   http://aka.ms/CyberPAW

2. Time-bound privileges (no permanent admins)  
   http://aka.ms/PAM  
   http://aka.ms/AzurePIM

3. Multi-factor for elevation

4. Just Enough Admin (JEA) for DC Maintenance  
   http://aka.ms/JEA

5. Lower attack surface of Domain and DCs  
   http://aka.ms/HardenAD

6. Attack Detection  
   http://aka.ms/ata

30 Days  >  90 Days  >  Beyond  
Build visibility and control of administrator activity, increase protection against typical follow-up attacks

[Diagram showing flow of administration and security measures]
Protecting Active Directory and Admin privileges

1. Modernize Roles and Delegation Model

2. Smartcard or Passport Authentication for all admins
   [Link](http://aka.ms/Passport)

3. Admin Forest for Active Directory administrators
   [Link](http://aka.ms/ESAE)

4. Code Integrity Policy for DCs (Server 2016)

5. Shielded VMs for virtual DCs (Server 2016 Hyper-V Fabric)
   [Link](http://aka.ms/shieldedvms)

Move to proactive security posture

30 Days  90 Days  Beyond
Roadmap for Securing Privileged Access

FIRST 30 DAYS
1. Separate Admin account for admin tasks
2. Privileged Access Workstations (PAWs) for Active Directory Admins
3. Unique Local Admin Passwords for Workstations
4. Unique Local Admin Passwords for Servers

FIRST 90 DAYS
5. Privileged Access Workstations (PAWs) for all admins
6. Time-bound privileges (no permanent admins)
7. Multi-factor for elevation
8. Just Enough Admin (JEA) for DC Maintenance
9. Lower attack surface of Domain and DCs
10. Attack Detection for Credential Theft (known attacks, UEBA)

Attack Demo
http://aka.ms/credtheftdemo
SPA Roadmap
http://aka.ms/SPARoadmap