Back to the Basics

Dr. Eric Cole

© 2014 Secure Anchor Consulting. All rights reserved.
Current Threat Level: RED
2Q 2014

• Current Risks:
  – Data Theft
  – Long term compromise
  – Command and control capability
  – Competitive advantage

• Current Threats:
  – Trusted Insiders
  – Supply Chain

• Current Vulnerabilities
  – Lack of segmentation
  – No data discovery
  – Systems not properly hardened
Myths About Attacks

• They only target governments
• Small organizations are not a target
• Destruction is the main goal
• The focus is on stealing information only
• Attackers want to take a piece of information and leave
Why Attacks are Successful?

- Organizations do not have security devices properly configured
- Not understanding the difference between a product and a solution
- Lack of data classification
- Not sufficient logging and correlation
- Too much visibility on the internal network
- Minimal asset management and configuration control
- Failure to institute least privilege
Prevention is Ideal
But
Detection is a Must
WHY?

PREVENT – DETECT – RESPONSE

Core to Success:
- Asset Inventory
- Configuration Management
- Change Control
- Segmentation
5 Steps to a Secure Future
Step 1: Identify Critical Data

Align critical assets with threats and vulnerabilities to focus on risk
Risk Based Thinking

1) What is the risk?
2) Is it the highest priority risk?
3) Is it the most cost effective way of reducing the risk?
Step 2: Align the Defense with the Offense

1) Reconnaissance
2) Scanning
3) Exploitation
4) Creating backdoors
5) Covering tracks
Step 3: Know thy Organization
If the offense knows more than the defense you will lose

Requirements:

a) Accurate up to date network diagram
b) Network visibility map
c) Configuration management and change control
You Cannot Protect What You Do Not Know About
Data Flow is Critical
Step 4: Defense in Depth

There is no such thing as an unstoppable adversary

Requirements:

a) Inbound prevention
b) Outbound Detection
c) Log correlation
d) Anomaly detection
Step 5: Common Metrics

Everyone must be using the same playbook in order to win

Requirements:

a) Utilize the critical controls
   i. Offense informing the defense
   ii. Automation and continuous monitoring of security
   iii. Metrics to drive measurement and compliance
<table>
<thead>
<tr>
<th>Critical Control</th>
<th>Effect on Attack Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Inventario de Dispositivos Autorizados y No Autorizados</td>
<td>Very High</td>
</tr>
<tr>
<td>2. Inventario de Software Autorizado y No Autorizado</td>
<td>Very High</td>
</tr>
<tr>
<td>3. Configuraciones seguras para Hardware y Software en Portátiles, Sistemas, y Servidores</td>
<td>Very High</td>
</tr>
<tr>
<td>4. Evaluación y Atención Continua de Vulnerabilidades</td>
<td>Very High</td>
</tr>
<tr>
<td>5. Defensas Malware</td>
<td>High</td>
</tr>
<tr>
<td>6. Seguridad del Software Aplicativo</td>
<td>High</td>
</tr>
<tr>
<td>7. Control de Dispositivos Inalámbricos</td>
<td>High</td>
</tr>
<tr>
<td>8. Capacidad de Recuperación</td>
<td>Moderadamente Alto a Alto</td>
</tr>
<tr>
<td>9. Evaluación de habilidades y capacitación apropiada para llenar brechas</td>
<td>Moderadamente Alto a Alto</td>
</tr>
<tr>
<td>10. Configuraciones seguras para Dispositivos de redales, Routers, y Switches</td>
<td>Moderadamente Alto</td>
</tr>
<tr>
<td>11. Control y Limitación de Puertos, protocolos, y servicios</td>
<td>Moderadamente Alto</td>
</tr>
<tr>
<td>12. Uso controlado de privilegios administrativos</td>
<td>Moderado a Moderadamente Alto</td>
</tr>
<tr>
<td>13. Defensa de la frontera</td>
<td>Moderado</td>
</tr>
<tr>
<td>14. Mantenimiento, monitoreo, y análisis de registros de auditoría de seguridad</td>
<td>Moderado</td>
</tr>
<tr>
<td>15. Acceso controlado basado en lo que se conoce</td>
<td>Moderado</td>
</tr>
<tr>
<td>16. Monitoreo y control de cuentas</td>
<td>Moderado</td>
</tr>
<tr>
<td>17. Prevención de pérdida de datos</td>
<td>Moderado a Bajo a Moderado</td>
</tr>
<tr>
<td>18. Capacidad de respuesta incidente</td>
<td>Moderado a Bajo a Moderado</td>
</tr>
<tr>
<td>19. Ingeniería de red</td>
<td>Bajo</td>
</tr>
<tr>
<td>20. Pruebas de penetración y ejercicios de equipo rojo</td>
<td>Bajo</td>
</tr>
</tbody>
</table>

**figure 1:** The 20 Critical Security Controls (Version 3.1) and Their Effect on Attack Mitigation
(Adapted from www.sans.org/critical-security-controls/winter-2012-poster.pdf)
Bottom Line....
It is time to take control of your data

Let’s stop making an easy target for the adversary
Winning at Cyber Defense

1) What is the risk?
2) Is it the highest priority risk?
3) Is it the most cost effective way of reducing the risk?
THANK YOU for your time

Dr. Eric Cole

Twitter: drericcole
ecole@secureanchor.com
eric@sans.org
www.securityhaven.com