Tackling Cybersecurity with Data Analytics

Identifying and combatting cyber fraud

San Antonio IIA | iHeartAudit Conference | February 24, 2017
What We’ll Cover

- Current threat landscape
- Common security measures
- Why this isn’t enough (case studies)
- How to identify the needle in the haystack
- What organizations should be doing
Presenters

Brett Nabors, CISA
Weaver
Senior Manager, IT Advisory Services

Reema Parappilly, CISA
Weaver
Senior Manager, Data Analytics
The comments and statements in this presentation are the opinions of the speakers and do not necessarily reflect the opinions or positions of Weaver and Tidwell, LLP.

This presentation is the property of Weaver and Tidwell, LLP. All rights reserved. No part of this document may be reproduced, transmitted or otherwise distributed in any form without written permission from Weaver and Tidwell, LLP.

Weaver and Tidwell, LLP expressly disclaims any liability in connection with the use of this presentation or its contents by any third party.
IT Advisory Services
DISTINGUISHING IT AS A STRATEGIC ADVANTAGE

IT Advisory Services (ITAS) is a collection of assurance and consulting services focused on information technology. We work with IT organizations, internal audit departments, security organizations and more.

**Resource Optimization**
- Software Selection
- Independent Verification & Validation
- IT Assessments & Planning
- IT Governance

**Risk Management**
- IT Risk Assessment
- IT Audit
- Project Risk Management
- Service Organization Control (SOC)

**Security & Availability**
- Information Security
- Data Privacy
- Business Continuity/Disaster Recovery

**Compliance**
- Payment Card Industry (PCI)
- Gramm-Leach Bliley
- Sarbanes-Oxley
- HIPAA
- FFIEC & FDICIA
Current Landscape
TWO KINDS OF ORGANIZATIONS:

1. those that have been breached

2. those that know that they’ve been breached
What’s going on

+ Zero day malware via phishing and websites
+ Gets past typical controls
+ Impact:
  – Data / system hijacking & ransom
  – Data exfiltration (credentials, account info, card info)
  – Fraudulent transactions, credit card fraud, identity theft, fraudulent wires, account takeover
Yahoo says data stolen from 1 billion accounts
What’s going on

By the numbers….

**May** – LinkedIn (167 million), Myspace (360 million)

**September** – Krebs – DDoS attack around 620-655 Gbps

**October** – Dyn DDoS – 20k IoT endpoints

**November** – AdultFriendFinder – 412 million

**December** – Yahoo – over 1 billion accounts
(from 2013, 2014)

DHS, FDIC, IRS,….
What’s going on

How fast is a gigabit internet connection?
What are they after?
Where does the data go?

Netflix Has Been Hacked, And Your Account Details Could Be Sold on the Dark Web

By Tommy DePaoli - Posted on December 4th, 2015 at 11:24am  Last edit on December 17th, 2015
Common Measures
What are we doing today?

- Anti-virus, anti-malware
- Patching updating
- Employee and customer training
- Perimeter security
- Scanning, vulnerability assessment, and penetration testing
- Social engineering assessments
- Some risk assessment & vendor management
What is accomplished?

- Identifying / fixing known issues
- Making it harder to attack us
- Educating our employees
What’s NOT accomplished?

+ Progress against zero day malware
+ Getting hands around the cyber risk
+ Ability to detect issues quickly
+ Resiliency, preparedness for when something happens
“Prevention is ideal, detection is a must!”
How Data Analytics Can Help You
TO BE ABLE TO ANALYZE DATA, YOU NEED TO BE LOGGING AND STORING THE DATA.
Tools

- Splunk
- Tripwire
- QRadar
Repurposing Existing Tools

- Internal Audit’s tool
- Utilized by IT
  - Proof of Concept
  - Ongoing tool
- Oversight by IA
  - Monitoring
Scenarios
Utilizing Tools

- Alerting
- Periodic Reviews
- Port Scans
- Unauthorized Connections
- Rejected IP Addresses
- Unsuccessful logins
- Outbound activity from internal servers
- Source routed packets
Scenarios

10/13/2015 5:42 PM, Info, 172.##.##.##, id = firewall
sn = # # # # # # # # # # # time = "2015-10-13 22:42:59 UTC"
fw = 174.##.##.## pri = # c = # # # m = # # #
msg = "Connection Closed" app = # # #
n = # # # # # # # # # # # src = 192.###.###.###:###:
V###: dst = 23.##.##.##:###:###: proto = tcp/https
sent = 1493 rcvd = 14873

<table>
<thead>
<tr>
<th>Field_2</th>
<th>COUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error</td>
<td>17</td>
</tr>
<tr>
<td>Debug</td>
<td>89</td>
</tr>
<tr>
<td>Alert</td>
<td>1806</td>
</tr>
<tr>
<td>Warning</td>
<td>3141</td>
</tr>
<tr>
<td>Notice</td>
<td>122944</td>
</tr>
<tr>
<td>Info</td>
<td>867001</td>
</tr>
</tbody>
</table>

<< End of File >>
### Scenarios

<table>
<thead>
<tr>
<th>Source IP Address</th>
<th>Destination IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>174</td>
<td>70.</td>
</tr>
<tr>
<td>175</td>
<td>207</td>
</tr>
<tr>
<td>176</td>
<td>66.</td>
</tr>
<tr>
<td>177</td>
<td>174</td>
</tr>
<tr>
<td>178</td>
<td>166</td>
</tr>
<tr>
<td>179</td>
<td>167</td>
</tr>
<tr>
<td>180</td>
<td>64.</td>
</tr>
<tr>
<td>181</td>
<td>40.</td>
</tr>
<tr>
<td>182</td>
<td>68.</td>
</tr>
<tr>
<td>183</td>
<td>192</td>
</tr>
<tr>
<td>184</td>
<td>172</td>
</tr>
</tbody>
</table>

### Protocols

<table>
<thead>
<tr>
<th>Protocols</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>udp/dns</td>
<td>460246</td>
</tr>
<tr>
<td>tcp/htt</td>
<td>151990</td>
</tr>
<tr>
<td></td>
<td>30155</td>
</tr>
</tbody>
</table>
Causation & Correlation

+ **Causation**: an act that occurs in such a way that something happens as a result

+ **Correlation**: a relationship between two variables

**Correlation does not imply causation**
Steps to Take
YOU PERSONALLY FACE GROWING LIABILITY FOR PROTECTING INFORMATION ASSETS

Executives and Directors are no longer viewed as innocent victims in the event of a cyber breach.

GROWING RISKS

+ New consumer protection laws hold officers accountable for cyber breaches.
+ State attorneys general now target organizations for non-disclosure of cyber breaches.
+ Improperly handled cyber attacks are now considered breaches of fiduciary duty.
Organizational Impact

A SINGLE BREACH COULD RESULT IN SEVERE ORGANIZATIONAL PROBLEMS

Cyber criminals now target trade secrets, intellectual property, and financials, as well as personal data.

POTENTIAL HARM

+ Lawsuits resulting from a breach can cost millions.
+ Incident response and remediation can result in significant expense.
+ Loss of public trust can damage organizational effectiveness
Call to Action

YOUR CURRENT TACTICS FOR CYBER SECURITY ARE NOT ENOUGH

Misconceptions and misinformation can leave you vulnerable and at risk.

FACTS

+ Continuous monitoring of cyber threats is now an essential practice.
+ Tools such as mobile devices open doors for cyber breaches.
+ Cyber crime methods and technology change and escalate daily.
+ Audits and Vulnerability Assessments are NOT enough
Preparing for Battle

Leveraging Cyber Threat Intelligence Proactively

+ Can you Respond to an incident?
+ Is there Zero-Day malware within our environment now?
+ What do the hackers currently have of mine?
Homeland Security says, “PPD-21 defines resilience as the ability to prepare for and adapt to changing conditions, and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.”
Cyber Resiliency (cont.)

1. Asset Management
2. Controls Management
3. Configuration and Change Management
4. Vulnerability Management
5. Incident Management
6. Service Continuity Management
7. Risk Management
8. External Dependency Management
9. Training and Awareness
10. Situational Awareness

https://www.us-cert.gov/ccubedvp/self-service-crr
Cyber Resiliency Resources

Downloadable Resources

CRR Self-Assessment Package

This package includes the entire CRR self-assessment, including the fillable assessment form and report generator. All assessments will require this file to be completed.

CRR Method Description and User Guide

This guide contains the overall description of the CRR along with detailed steps and explanations for how to conduct a CRR self-assessment at an organization.

CRR Question Set with Guidance

This document contains the entire CRR self-assessment question set along with guidance on how to interpret and answer each of the questions contained within the self-assessment package.

CRR NIST Framework Crosswalk

This document provides a cross-reference chart for each of the categories in the NIST Cybersecurity Framework and how they align to the CRR and other references.

CRR Information Sheet

This is a brief fact sheet on the CRR summarizing the process.

https://www.us-cert.gov/ccubedvp/self-service-crr#
On January 10, 2017, NIST released proposed updates to Cybersecurity Framework [link to new page]. This draft Version 1.1 of the Cybersecurity Framework seeks to clarify, refine, and enhance the Framework. Updates were derived from feedback NIST received since publication of Cybersecurity Framework Version 1.0, including responses to a December 2015 RFI entitled Views on the Framework for Improving Critical Infrastructure Cybersecurity and discourse at Cybersecurity Framework Workshop 2016.


SANS 20 Critical Security Controls

Control 1: Inventory of Hardware Devices
Control 2: Inventory of Software
Control 3: Secure Configurations for Computer Systems
Control 4: Vulnerability Assessment and Remediation
Control 5: Malware Defenses
Control 6: Application-Layer Software Security
Control 7: Wireless Device Control
Control 8: Data Recovery Capability
Control 9: Skills Assessment and Training
Control 10: Secure Configurations for Network Devices
Control 11: Control of Network Ports, Protocols and Services
Control 12: Administrative Privileges
Control 13: Boundary Defense
Control 14: Audit Logs
Control 15: Controlled Access Based on Need To Know
Control 16: Account Monitoring and Control
Control 17: Data Loss Prevention
Control 18: Incident Response
Control 19: Secure Network Engineering
Control 20: Penetration Tests
Questions?