Nonprofit Cybersecurity Incident Report

TechForward #Secured

September 2019
About Community IT

100% Employee Owned

Advancing mission through the effective use of technology.
NONPROFIT CYBERSECURITY INCIDENT REPORT
<table>
<thead>
<tr>
<th>Agenda</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>Cybersecurity landscape</td>
</tr>
<tr>
<td>Our approach to cybersecurity</td>
</tr>
<tr>
<td>Types of incidents</td>
</tr>
<tr>
<td>Report data</td>
</tr>
<tr>
<td>Engage your leadership</td>
</tr>
<tr>
<td>Secure your organization</td>
</tr>
</tbody>
</table>
CYBERSECURITY LANDSCAPE

- Persistent and ongoing brute force attacks on identities
- Sophisticated spear phishing
- Organizations targeted because of the work they do
- Attacks targeting vendors
New security tools available to combat new threat types.

Organization’s starting to ask about where to start in improving their cybersecurity.

68% of Nonprofits don’t have an Incident Response Plan

Breach response for a small to medium business is $149,000
Cybersecurity - Adversaries
Cybersecurity Landscape

Attack Vectors Commonly Used in Ransomware Incidents: Q2 2019

- Email Phishing: 34.1%
- RDP Compromise: 59.1%
- Software Vulnerability: 6.8%

https://www.coveware.com/blog/2019/7/15/ransomware-amounts-rise-3x-in-q2-as-ryuk-amp-sodinokibi-spread
1.5 Million RDP Servers Attacked
OUR APPROACH TO CYBERSECURITY

NextGen Tools

IDENTITY  DATA  DEVICES  PERIMETER  WEB

SECURITY AWARENESS

SECURITY POLICY
Incident

An event that compromises the integrity, confidentiality or availability of an information asset.
Breach

An incident that results in the confirmed disclosure—not just potential exposure—of data to an unauthorized party.
NONPROFIT CYBERSECURITY INCIDENT REPORT 2018

February 2018, 1st Edition

© 2018 Community IT Innovations, Inc. All rights reserved.

BASELINE INFRASTRUCTURE SECURITY PRACTICES

In anticipation of providing some results for the public, we are happy to provide information about the steps that have been taken to improve the cybersecurity posture of our organization. We have implemented a number of practices to help ensure the security of our infrastructure.

INTEGRITY AND ACCESS CONTROL

We have established a clear set of policies and procedures to control access to our systems. These policies include the assignment of access rights based on job responsibilities and the enforcement of strong password policies.

BASIS INFRASTRUCTURE SECURITY PRACTICES

We have implemented a number of practices to strengthen the security of our infrastructure. These practices include the use of firewalls, intrusion detection systems, and security awareness training for all employees.

INCIDENT RESPONSE

We have established a comprehensive incident response plan to ensure that we can quickly respond to any security incidents that may occur.

CYBERSECURITY INCIDENTS

The table below provides a summary of the types of incidents that were reported in 2018.

<table>
<thead>
<tr>
<th>INCIDENT TYPE</th>
<th>COUNT OF INCIDENTS</th>
<th>COUNT OF SAMPLE</th>
<th>% OF TOTAL INCIDENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing</td>
<td>15</td>
<td>25</td>
<td>30%</td>
</tr>
<tr>
<td>Malware</td>
<td>10</td>
<td>20</td>
<td>30%</td>
</tr>
<tr>
<td>Ransomware</td>
<td>5</td>
<td>10</td>
<td>15%</td>
</tr>
<tr>
<td>SQL Injection</td>
<td>3</td>
<td>6</td>
<td>10%</td>
</tr>
<tr>
<td>Botnet</td>
<td>2</td>
<td>4</td>
<td>6%</td>
</tr>
<tr>
<td>Cross Site</td>
<td>1</td>
<td>2</td>
<td>3%</td>
</tr>
<tr>
<td>Cross Domain</td>
<td>1</td>
<td>2</td>
<td>3%</td>
</tr>
<tr>
<td>Cross Network</td>
<td>1</td>
<td>2</td>
<td>3%</td>
</tr>
<tr>
<td>Cross Service</td>
<td>1</td>
<td>2</td>
<td>3%</td>
</tr>
<tr>
<td>Malware</td>
<td>1</td>
<td>2</td>
<td>3%</td>
</tr>
<tr>
<td>SQL Injection</td>
<td>1</td>
<td>2</td>
<td>3%</td>
</tr>
<tr>
<td>Botnet</td>
<td>1</td>
<td>2</td>
<td>3%</td>
</tr>
<tr>
<td>Cross Site</td>
<td>1</td>
<td>2</td>
<td>3%</td>
</tr>
<tr>
<td>Cross Domain</td>
<td>1</td>
<td>2</td>
<td>3%</td>
</tr>
<tr>
<td>Cross Network</td>
<td>1</td>
<td>2</td>
<td>3%</td>
</tr>
<tr>
<td>Cross Service</td>
<td>1</td>
<td>2</td>
<td>3%</td>
</tr>
</tbody>
</table>

This table shows that phishing and malware incidents were the most common types of incidents reported in 2018. Phishing incidents constituted 30% of the total number of incidents, while malware incidents constituted 30% of the total number of incidents.
Types of incidents

• **Email Phishing**: a social engineering attack that attempts to get a user to click on a link that goes to a malicious site that contains malware or steals credentials

• **Malware**: any type of malicious software, usually reported by the end user as a slow computer or strange pop-ups

• **Account Compromise**: unauthorized use of a digital identity by someone other than the assigned user
Types of incidents

- **Business Email Compromise**: scam using traditional confidence scheme techniques combined with email impersonation to extract funds through illicit means
- **Wire Fraud**: any fraudulent or deceitful scheme to steal money by using phone lines or electronic communications through electronic means
- **Virus**: a malicious piece of software that can alter the way a computer works, typically spread from one computer to another, often rendering the computer and/or data unusable
Types of incidents

• **Supply Chain:** an attack that is initiated through a partner of the organization. Also known as a value-chain or third-party attack.

• **Advanced Persistent Threat:** State-Sponsored actor or criminal group focused on targeting a specific organization or individual, operating over a long period of time with a goal of remaining undetected and exfiltrating data.

• **Ransomware:** a type of virus that has the characteristic of encrypting files and then demanding payment for decrypting the files.
<table>
<thead>
<tr>
<th>INCIDENT TYPE</th>
<th>COUNT OF INCIDENTS</th>
<th>COUNT OF SAMPLE</th>
<th>% OF SAMPLE EXPERIENCE INCIDENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Email Phishing</td>
<td>140</td>
<td>41</td>
<td>26%</td>
</tr>
<tr>
<td>2. Malware</td>
<td>54</td>
<td>39</td>
<td>25%</td>
</tr>
<tr>
<td>3. Account Compromise</td>
<td>20</td>
<td>18</td>
<td>12%</td>
</tr>
<tr>
<td>4. Business Email Compromise</td>
<td>14</td>
<td>13</td>
<td>8%</td>
</tr>
<tr>
<td>5. Wire fraud</td>
<td>3</td>
<td>3</td>
<td>2%</td>
</tr>
<tr>
<td>6. Virus</td>
<td>1</td>
<td>1</td>
<td>1%</td>
</tr>
<tr>
<td>7. Advanced Persistent Threat</td>
<td>1</td>
<td>1</td>
<td>1%</td>
</tr>
<tr>
<td>8. Supply Chain</td>
<td>0</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>9. Ransomware</td>
<td>0</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td><strong>Grand Total</strong></td>
<td><strong>233</strong></td>
<td><strong>116</strong></td>
<td><strong>50%</strong></td>
</tr>
</tbody>
</table>
Year to date trends

Year over Year Comparison

• Volume of reported spam increased
• Business Email Compromise has spiked
• Account compromises holds steady, even among increasing MFA adoption
• Wire Fraud has increased
• Actual virus infection rate is low
• Ransomware in sample is low
Analysis of Our Data and Sector

• Spearphishing / Business Email Compromise is increasing
• Supply chain attacks up dramatically in our sector
  • Vendor -> Client
  • Org -> Org
• Security Awareness Training adoption is increasing
• MFA adoption is increasing
• We still have a long way to go
MFA is Effective

Account takeover prevention rates, by challenge type

<table>
<thead>
<tr>
<th>Challenge Type</th>
<th>Device-based challenges</th>
<th>Knowledge-based challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-device prompt</td>
<td>100%</td>
<td>73%</td>
</tr>
<tr>
<td>SMS code</td>
<td>100%</td>
<td>79%</td>
</tr>
<tr>
<td>Security key</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td>Secondary email address</td>
<td>99%</td>
<td>68%</td>
</tr>
<tr>
<td>Phone number</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td>Last sign-in location</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

Legend:
- Blue: Automated bot
- Red: Bulk phishing attack
- Orange: Targeted attack
- Gray: 95% confidence interval
Knowledge into Action
Engage your Leadership

All organizations are vulnerable

Poor cybersecurity is an organizational liability

Requires leadership to say yes
Engage your Leadership

Schedule
- Schedule time for cybersecurity
  - Monthly reporting
  - Quarterly planning

Know
- Know your audience
  - Narrative
  - Metrics and numbers

Leverage
- Leverage existing compliance requirements
  - PCI
  - HIPAA
  - GDPR
Cybersecurity Readiness

<table>
<thead>
<tr>
<th>People</th>
<th>Process</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Passwords</td>
<td>• Policy</td>
<td>• Antivirus</td>
</tr>
<tr>
<td>• MFA</td>
<td>• Security Awareness Training</td>
<td>• Backup</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Email Protection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Etc..</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Getting Started with Cybersecurity

- IT Policy
- Security Awareness Training
- OS and Third Party Updates
- Antivirus
- Backups
- MultiFactor Auth
- Business Email Compromise Protection
Growing Organization

- BIOS / Driver Updates
- Web Filtering
- BYOD Control
- Device Encryption
- Endpoint Detection and Response
- Risk Assessment
Mature/Compliant Organization

- Cyberliablity Insurance
- Cybersecurity Assessment
- SOC / SIEM
- Vulnerability Scanning
- Penetration Testing
NIST Risk Assessment Tool
Resources

- [https://www.sans.org/security-resources/policies/](https://www.sans.org/security-resources/policies/)
- NIST Assessment Tool
  - Email [meshleman@communityit.com](mailto:meshleman@communityit.com) for free access
THANK YOU!