Defending Your Business Against Cybersecurity Threats

Kevin T. Smith, Tridium
Read The News Lately?

Yahoo says 500 million accounts stolen
by Seth Fiegelman @sfiegelman
September 23, 2016 10:39 AM ET

Yahoo: Hackers Stole Data On Another Billion Accounts released every day
by Victoria Harrison and Jose Padilla @CNNTech

FBI investigates cyber attack on Democratic National Committee
Up to 400 million accounts infected in Finder breach

Here Are 4 Vulnerabilities Ransomware Attacks Are Exploiting Now
A zero-day exploit was used to breach a company
Another Day, Another New Threat to the Internet

Bought a car recently? Millions of dealership customer details found online
Customers for more than a hundred car dealerships across the US were put at risk because of shoddy database security.

FBI issues IoT security warning

An Army of Million Hacked IoT Devices Almost Broke the Internet Today

Risk Assessment
Double-dip Internet-of-Things botnet attack flaw leaves the Internet

Data privacy risks
In front of the telly: Warning over 'big' TV

Is Britain, Europe and hit by 'Petya' ransomware attack with chilling echoes of 'Cry' assault which crippled

Takes Down Central Heating
31st Winter in Finland

DEFCON 2.0: Expert warns cyber warfare reached critical turning point
More than 65m Tumblr emails for sale

Industrial control systems a growing target for cyber attack

FBI: An Account on Clinton’s Private Email Server Was Hacked

Microsoft Office 365 Users Targeted in Brute Force Attacks
Agenda

• Understanding the Threats
• Defending Against the Threats
• Top 10 Best Practices – 2017 Edition
The Effect of a Breach on Cost & Trust

$3.62 million
Average cost of ONE data breach in the US
(not including revenue losses due to lost business)
- IBM/Ponemon Institute Research Report, 2017

Equifax’s stock has fallen 31% since breach disclosure, erasing $5 billion in market cap

By Victor Reklaitis
Published: Sept 14, 2017 6:25 a.m. ET
The IoT – A New Frontier for Hackers

‘Internet Of Things’ Hacking Attack Led To Widespread Outage Of Popular Websites

October 22, 2016 - 8:10 AM ET
Heard on Weekend Edition Saturday

How IoT hackers turned a university’s network against itself

A university found its own network turned against it - as refrigerators and lights overwhelmed it with searches for seafood.

Watch This Building's Smart Lights Get Hacked by a Drone

Got a few days and a couple hundred bucks? That's enough to do some pretty flash hacking.

DDoS Attack Takes Down Central Heating System Amidst Winter In Finland

Wednesday, November 09, 2016  Mohit Kumar

"If your industrial control system is connected to the Internet, it has almost a 100 percent guarantee to be hacked the first day.”

— E. Kaspersky, founder, Kaspersky Lab

Tucson digital traffic sign hacked, July 2015

#internetOfthingsIWantToHack
Connected Devices: “Hacked in minutes”

USA Today/Avantgarde Cyber Security Study:

• 6 PCs were directly connected to the Internet
• 305,922 attacks, beginning instantly
• Intruder successfully broke in within 4 minutes
• Machines w/ security patches attacked the least
• Most attacks were automated (BOTS, not live hackers)

“Unprotected PCs Can Be Hijacked in Minutes”
USA Today
Shodan and Other “Hacker Friendly” Sites

They can find you...

The search engine for Buildings
Shodan is the world’s first search engine for Internet-connected devices.

Explore the Internet of Things
Use Shodan to discover which of your devices are connected to the Internet, where they are located, and who is using them.

Monitor Network Security
Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

And ruin your day.

Oops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so much time.

Get a Competitive Advantage
Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am.

Send $300 worth of bitcoin to this address:

12d9YDPgwueZ3NyMgw669B7AAl6xjr65Mw

Check Payment Decrypt
“If you talk to these companies, they’ll swear up and down that their controller networks are “isolated” from other computer networks, including the Internet. But many, many times, there’s a connection that the engineers are not aware of...”

“Cyber Risk Isn’t Always in the Computer,” Seth Bromberger, WSJ, Sept 24, 2015
Attacking Internet-exposed Devices

1. Bad Guy searches for device on shodan, censys, zoomeye
   • Are you visible on the Internet?
2. Tries previously published vulnerabilities, old default passwords
   • Are you current with all security patches?
   • Do any of your devices use factory-default passwords?
   • Do you use easy-to-guess passwords?
3. Attempts to log on to device
4. Attempts to flood device with packets to cause Denial of Service

Successful attacks result in “owning your building,” crashing your system, and/or going farther into your network to attack other things
Ransomware on the Rise!

- In the 6 months of June – November 2016, nearly one billion total malware incidents were reported.
  - Ransomware was found to be 66% of All Malware, increasing by 267% in 2016 – “An Unprecedented Domination of the Threat Landscape” – Malwarebytes, 2017
- FBI: $209 million was extorted in Q1 2016 alone – CNN, April 2016
- Symantec: Average number of ransomware infections fluctuated between 23,000 and 35,000 per month, with a spike in 56,000 in March 2016
- Email is the #1 Delivery Vehicle (link, attachment)
- Web Site is the #2 Delivery vehicle

*Image – Santeri Viinamake, Creative Commons

Do you check email or surf the web from mission critical infrastructure? If so, your mission-critical systems could be vulnerable to Ransomware attacks.

TRIDION®
Defending Against the Threats: Organizational Best Practices
What Impacts Your Building’s Security?

1. Security Configuration of your network
   (IT departments)

2. Built-in capabilities of your connected products
   (Vendor)

3. What ELSE is connected to your network?
   (IT departments, End Users, “Shadow IT”)

4. Configuration of your connected products
   (Integrators, Administrators)

5. How Are Your Products Being Used?
   (End Users)

6. Is Your Network Segmented with Defense-In-Depth Principles?

7. What are your connected products?

8. How Secure Are They?

9. And what are THEY connected to?
   (external connections, cloud services, other networks)

10. How Cyber-Aware are your integrators?

11. How Cyber-Aware are your end-users?

If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology. -Bruce Schneier
The Evolution of Intelligent Buildings
People, Processes & Technology

- Security isn’t just an “IT thing”
- Policies and procedures are critical
  - Patch management
  - Proper use of IT systems
  - Proper use of building control systems
  - Procedures for incident response
- Communicate: Make sure users understand/respect the cyber threat and follow organizational security policies
- Educate: Teach them how to follow the correct procedures
- Enforce: Make sure everyone knows that Cybersecurity is a priority from the top down in your organization & enforce good behavior through technical controls where possible.
IT & OT: “We need to talk.” (and change).

- Too often, IT and Facilities don’t communicate, and things become connected without organizational oversight.
- “Shadow IT”: Connecting systems to the network without IT’s knowledge.
- The IT department’s job is to secure mission-critical assets on the network.
- All aspects of building control systems are mission-critical!

*Cybersecurity Threats & Concerns must drive organizational change.*
What We’re Doing: Security in Niagara 4

- Making security easier through “secure by default” principle:
  - Forcing default credential changes immediately upon commissioning
  - Strongest authentication mechanism by default
  - Enforcement of strong passwords
  - Encrypted communications (FoXS and HTTPS)
- Role-based access control
- Encryption of sensitive information at rest
- “Sandboxing”: Authorization at the Code Level
- Digitally signed code validated for integrity at run time
- JACE® 8000 secure boot

As we evolve our product architecture, we will continue to use the approach of “secure by default” and enforcing good cyber behavior through technology controls.
1. NEVER Expose your Building on the Internet

Do Your Internal Devices Actually Need to Be Connected to the Internet?

- Determine your organization’s appetite for risk.

For Cloud Access:

- Never use a Cloud solution that requires incoming connection from the Internet.
- Never allow incoming connections to your devices.

For Remote Access to Your Device:

- Consider a security gateway that acts as a VPN server as part of your network security solution
- Put your assets behind the security gateway
- Devices behind security gateway are concealed from Internet discovery; All transmissions encrypted

For more information on securely connecting Niagara, see:
- Niagara 4 and AX Hardening Guides
- Using a VPN with Niagara Systems

Find them at www.tridium.com/en/resources/library
2. Use a Defense-In-Depth Network Security Strategy

From “Recommended Practice: Improving Industrial Control Cybersecurity With Defense-In-Depth Strategies”

DHS, ICS-CERT, 2009
3. Always Change “Factory Default” Credentials on Devices within your Building’s Network.
4. Execute a Patch Management Plan

- Organizations such as US-CERT and ICS-CERT provide a great service internationally, reporting vulnerabilities in hardware and software.
- Many advisories affect millions of devices.
- Vendors release security patches and updates, and these organizations point you to where to get them.
- *Any* unpatched system on your network can be an attacker’s avenue into your organization.

TIP: NIST SP 800-40r3 Provides Guidance for Patch Management for Your Organization that can be helpful for all building systems (control systems, edge devices, etc.).
5. Protect Yourself from Ransomware

1. Educate your people on the safe use of IT assets and the dangers of ransomware
2. Use anti-virus software on your systems and keep them up to date
3. Do periodic, scheduled backups of your systems
4. If you have a supervisory system (ex: Niagara Supervisor), treat it as mission-critical infrastructure, which means it shouldn’t be a “web surfing” or “email checking” machine

*Image – Santeri Viinamake, Creative Commons
6. Always use Encrypted Communications

<table>
<thead>
<tr>
<th>Hardening Guides</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Niagara AX Hardening Guide</td>
</tr>
<tr>
<td>• Niagara 4 Hardening Guide</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2017 Technical Bulletins</th>
</tr>
</thead>
<tbody>
<tr>
<td>• July 12: Recent ransomware and malware outbreaks</td>
</tr>
<tr>
<td>• May 17: Ransomware “WannaCry” Cyberattack Update</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2016 Technical Bulletins</th>
</tr>
</thead>
<tbody>
<tr>
<td>• June 27: Resolution for Niagara weather service-related issue</td>
</tr>
<tr>
<td>• June 17: Temporary workaround available for Niagara weather service-related issue</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2015 Technical Bulletins</th>
</tr>
</thead>
<tbody>
<tr>
<td>• August 7: Niagara AX 3.6, 3.7 and 3.8 updates</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2014 Technical Bulletins</th>
</tr>
</thead>
<tbody>
<tr>
<td>• October 21: Poodle Vulnerability</td>
</tr>
<tr>
<td>• September 30: Shellshock Security Bug</td>
</tr>
<tr>
<td>• July 25: Patch Available for Oracle Java 7, Update 65</td>
</tr>
<tr>
<td>• July 18: Tridium Working to Resolve issue Regarding Oracle Java 7 Update 65</td>
</tr>
<tr>
<td>• April 10: Open SSL</td>
</tr>
</tbody>
</table>

Niagara 4 Hardening Guide

Tips to Secure a Niagara 4 System

Cybersecurity and the IoT—Threats, Best Practices and Lessons Learned
Kevlin T. Smith, Chief Architect, Tridium
8. Don’t Forget Physical Security

- Even if you have great network security, secure products, it really doesn’t matter if someone can gain physical access to your control systems and edge devices.
- Remember that many successful cyberattacks can also begin with a physical one.
- Remember that malware can also be introduced through USB drives.
9. Do Periodic Risk Assessments

- Understand your organization’s appetite for risk & determine a risk threshold, re CVSS score
- Identify the electronic assets you wish to protect & document security requirements re: confidentiality, integrity, availability
- Engage an independent security team to assess threats and potential vulnerabilities for your network & those assets
- Follow up with action items
- Do this on a periodic basis – assets change, requirements change.
People are the most critical aspect of your organization’s security.
## Helpful Resources

<table>
<thead>
<tr>
<th>Resources</th>
<th>Where to find it</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIST SP 800-50: Building an Information Technology Security Awareness and Training Program</td>
<td><a href="http://www.nist.gov/">http://www.nist.gov/</a></td>
</tr>
</tbody>
</table>
Thank You!

Kevin T. Smith, CISSP, CSSLP
Chief Architect

ksmith@tridium.com
www.linkedin.com/in/kevintsmith/

www.tridium.com/en/resources/events