Defense in Depth

Creating Effective Layers of CyberSecurity to Protect Your Stores
Defense in Depth
Creating Effective Layers of CyberSecurity to Protect Your Stores

Hosts: Allie Russell & Jenny Bullard
arussel@conexxus.org
jbullard@conexxus.org

Moderator: Kara Gunderson
Chair, Data Security Committee
POS Manager, CITGO Petroleum
kgunder@citgo.com

Presenters:
Brett Stewart
CTO, Acumera
brett.stewart@Acumera.net
DeWayne Mangan PCIP, ISA
Director of Infrastructure, Acumera
dewayne.mangan@Acumera.net
Mark Palmer  PCIP, ISA, QIR
Director of Technical Solutions, Acumera
mark.palmer@Acumera.net

Conexxus
solve forward
Agenda

• Housekeeping
• About Conexxus
• Presentation
• Q & A
Housekeeping

This webinar is being recorded and will be made available in approximately 30 days.

• YouTube (youtube.com/conexxusonline)
• Website Link (conexxus.org)

Slide Deck
• Survey Link – Presentation provided at end

Participants
• Ask questions via webinar interface
• Please, no vendor specific questions

Email: info@conexxus.org
About Conexxus

• We are an independent, non-profit, member driven technology organization
• We set standards...
  • Data exchange
  • Security
  • Mobile commerce
• We provide vision
  • Identify emerging tech/trends
• We advocate for our industry
  • Technology is policy
# 2019 Conexxus Webinar Schedule*

<table>
<thead>
<tr>
<th>Month/Date</th>
<th>Webinar Title</th>
<th>Speaker</th>
<th>Company</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 24, 2019</td>
<td>Managed Detection and Response</td>
<td>Tom Callahan, Mark Carl</td>
<td>ControlScan</td>
</tr>
<tr>
<td>February 2019</td>
<td>PCI DSS for Petro Merchants</td>
<td>Elizabeth Terry</td>
<td>PCI SSC</td>
</tr>
<tr>
<td>March 2019</td>
<td>Defense In Depth: Creating Effective Layers of CyberSecurity to Protect Your Stores</td>
<td>Mark Palmer, DeWayne Mangan, Brett Stewart</td>
<td>Acumera</td>
</tr>
<tr>
<td>April 2019</td>
<td>Don’t get Phished! Train Your Employees to Avoid Ransomware</td>
<td>Geoffrey Vaughan, Ed Adams</td>
<td>Security Innovation</td>
</tr>
<tr>
<td>May 2019</td>
<td>Firewall compliance! The basics, the benefits, and the security</td>
<td>Simon Gamble</td>
<td>Mako Networks</td>
</tr>
<tr>
<td>June 2019</td>
<td>TBD</td>
<td>David Ezell, Ian Jacobs</td>
<td>Conexxus W3C</td>
</tr>
</tbody>
</table>
## 2019 Conexxus Webinar Schedule*

<table>
<thead>
<tr>
<th>Month/Date</th>
<th>Webinar Title</th>
<th>Speaker</th>
<th>Company</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 2019</td>
<td>Skimming</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td>August 2019</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td>September 2019</td>
<td>Updated Data Science Presentation</td>
<td>Ashwin Swamy Thomas Duncan</td>
<td>Omega ATC Omega ATC</td>
</tr>
<tr>
<td>November 2019</td>
<td>Outdoor EMV</td>
<td>Brian Russell Linda Toth</td>
<td>Verifone Conexxus</td>
</tr>
<tr>
<td>December 2019</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
</tr>
</tbody>
</table>
Conexxus thanks our 2018 Annual Diamond Sponsors!
Defense in Depth

Creating Effective Layers of CyberSecurity to Protect Your Stores
Defense-in-Depth Presentation Topics

• DiD defined, aka “layered approach”

• Three threat scenarios
  1. IoT Attack Vector
  2. Phishing Attack Vector
  3. Remote Vendor Access Attack Vector

• Summary

• Questions
Is your store network a box of bon-bons?

If you have a single layer of cybersecurity defense, think of that as a thin hard shell, with all the sweet stuff available anywhere you pierce that shell.
Or is it an onion?

If your network is an onion, there are many layers of defense* before critical assets are reached.

- References in [ ] are to the relevant section of the PCI DSS
“Defense in Depth” (aka “Layered Approach”)

“Defense in Depth” is the use of multiple computer security techniques to mitigate the risk of one component of defense being compromised or circumvented.

An example could be anti-virus software installed on individual workstations when there is already virus protection on the firewalls and servers.

Different security products may be deployed to defend different potential vectors within the network, reducing the chance a shortfall in any one defense could leading to a wider failure.
Defense in Depth of limited value without....

“Defense-in-depth needs to encompass ... both visibility and continuous monitoring. After all, you can’t secure what you can’t see. Without insight and visibility, the veritable castle walls of cyber defense will continue to have gaping holes and attackers will continue to leap through these holes and storm the castle.”

Julie Cullivan, CIO, ForeScout

[10,11,12]
Three Relevant Attack Vectors, discussed...

• IoT devices, like DVRs, ATGs, Frozen Barrel Machines, etc
• Employee web browsing
• Remote access to devices, especially the POS
IoT Device Security: Conexxus Resources

Internet of Things and Bring Your Own Device in your Business

Presenter: Jeff Gibson, ControlScan

Link
"Internet of Things" (IoT) in your store...

- Tank Gauge
- Video Camera
- ATMs
- Menu Boards
- Safe
- Overhead Music Player
...
Breach Vector: “IoT” in the store

“What confidence do you have that your IoT network is secure?”

70% Highly confident

“If audited, how confident do you think your organization could identify 100% of the IoT connected devices or solutions being used?”

18% Fully confident

Satisfaction with current IoT security is high, but doesn’t hold up when truly tested.
Why be concerned about IoT devices?

Cyber Criminals suborn an IoT device, then use it to launch a more concerted attack on higher-value targets like POS, resulting in:

• Loss of customer trust
• Loss of customer data
• Damage to brand name
• Fines related to losses
Example IoT Vulnerability

Over 5K Gas Station Tank Gauges Sit Exposed on the Public Net

It's been three years since researchers first discovered automated tank gauges (ATGs) at some 5,000 US gas stations exposed on the public Internet without password protection, and a recent scan found 5,635 locations were vulnerable to the same issue.

[Link]
Defend the ATG

- Awareness – Employee training
- Physical – Lock the backroom!
- Restrict connection to Internet
- Use anomaly-detecting IDS
- Place the ATG in it’s own segment
- Disable default access (pw protect)
Video Cameras Exploited

• Sophos researchers claim to have found 540,000 exploitable cameras.

Pixelated image at right was originally 4K HD, with Card Data easily visible

Link
Defend the DVR

- Awareness – Employee training
- Physical – Lock the backroom!
- Restrict connection to Internet
- Use anomaly-detecting IDS
- Place the DVR in it’s own segment
- Disable default access (pw protect)
Secret Service Warns of Sophisticated ATM Jackpotting Attack

(Washington, D.C.) – On this date, The United States Secret Service issued warnings to financial institutions about cyberattacks on ATM’s known as “jackpotting.”

ATM jackpotting is a sophisticated crime in which thieves install malicious software and/or hardware at ATMs that force the machines to dispense huge volumes of cash on demand. To execute a jackpotting attack, perpetrators must gain physical access to the cash machine and install malware, or specialized electronics, or a combination of both to control the operations of the ATM.

Criminals have been able to find vulnerabilities in financial institutions that operate ATM’s, primarily ATM’s that are stand-alone. The targeted stand-alone ATMs are routinely located in pharmacies, big box retailers, and drive thru ATMs. Criminals range from individual suspects to large organized groups, from local criminals to international organized crime syndicates.
Defend the ATM – Just the basics!

Recommendation for countermeasures

Diebold Nixdorf understands the impact of this threat and supports customers in identifying and deploying potential solutions. From a holistic security approach, Diebold Nixdorf recommends implementing the following countermeasures:

1) Limit Physical Access to the ATM
   - Use appropriate locking mechanisms to secure the head compartment of the ATM.
   - Control access to areas used by personnel to service the ATM.
   - Implement access control for service technicians based on two-factor authentication.
IoT Device Attack Vector

• The PCI DSS offers a great list of controls – implement them!

• Ask your IT department or network vendor
  • Can you visualize ALL devices attached to my network?
  • How quickly can you detect/isolate a rogue device?
  • Can you place protective remote access layers in front of devices like ATGs and DVRs?
  • Are you providing an IDS that detects anomalous network traffic patterns?
  • Are all the IoT devices on a different segment than Cardholder data?
  • What do you do (MDR) when something happens?
WannaCry and other Ransomware—Strategies and Approach for Preventing and Removing It

Presenter: George Sconyers, Omega ATC
Employee Browsing

• More than just **time management** concerns
• **Multiple** points of access (manager’s workstation, training machines, time clock consoles, multi-purpose tablets, etc)
• **Just clicking on a malicious link** is enough to infect a machine
• Advanced Persistent Threats (APTs) hide activity from users and are only detectable at a network level
Why be concerned with Employee Browsing?

• **One in 61 emails** in your inbox now contains a malicious link (Link)
• **4% of people** will click on any given phishing campaign (Link)
• Phishing in the news:
  
  Fake [Dun & Bradstreet Company Complaint](#) delivers Trickbot
  
  A reminder about [government-backed phishing](#) (Google)
  
  North Korean hackers [go on phishing expedition](#) before summit
  
  Top phishing subject line of 2018 [relates to password changes](#)
Employee Browsing - Example

Google Chrome **Zero-Day** Exploit - March 2019
(**CVE-2019-5786**)

“It appears to exploit this vulnerability, all an attacker needs to do is [trick] victims into just opening, or redirecting them to, a specially-crafted webpage **without requiring any further interaction.**” [Link](#)
LinkedIn Direct Messages Exploited Via “more_eggs” Backdoor

“...the threat actors began the phishing attack via LinkedIn DM by sending fake job offers. They then reach the recipient users by emails as follow-up reminders. **These emails contain malicious URLs that redirect the victims to legit-looking websites.**” [Link](#)
Additional Layers of Protection for Browsers

• Awareness Training!

• WebFilter
  • Use whitelisting
  • Use categories to augment whitelisting strategy
  • Apply to entire network

• IDS
  • Threat intel feeds to augment firewall rules
  • Pre-determined Managed Detection & Response plan

• Segmentation
  • Isolation & evaluation of HQ access needs
Basic Browsing with No Web Filter

1. Look up name on DNS server
2. DNS server returns IP address
3. IP address is referenced
4. Malware now on Computer
Browsing with Web Filter – Everything is checked

1. Reliable DNS by WebFilter
2. Phish site is resolved
3. Access is blocked
4. Alarm is raised
Important Web Filter Benefits

Restrict by Category

Explicitly Grant Access to Domains
Defend Business Browsing

Next Conexxus Webinar offers advice for people and process defense layer.

Physical – Lock the manager’s office!
Perimeter Security
  Web Filter
  IDS
Segmentation
  Segment away from Cardholder Data
Browsing Device Attack Vector

• The PCI DSS offers a great list of controls – implement them!
• Watch the upcoming Phishing Awareness Webinar
  • Phishing still a very common and effective vector
• Ask your IT department or network vendor
  • Can you divert all browsing to a webfilter?
  • How quickly can you detect/isolate an attack?
  • What do you do (MDR) when something happens?
• Are all the browsing devices on a different segment than Cardholder data?
• Are you providing an IDS that notes anomalous network traffic?
Remote Access: Conexxus Resources

Remote Access Compliance & Responsibilities
December 21, 2017
Version 1.0
Why the concern about Remote Access?

- Because so many breaches happen this way
Famous breaches with a remote access vector

Breached
- Third-party HVAC company opened virus-laden email attachment
- ~40M card numbers stolen
- Validated as “PCI-compliant” 2 months before the breach

Breached
- Stolen third-party vendor credentials then malware installed
- ~56M card numbers stolen
- Preventative MS Windows security update was available but had not been installed
Huddle House Breached This Way In February

Huddle House Data Breach Linked to Malware in the POS

02/05/2019

Malware that infected the point-of-sale system at some of Huddle House’s corporate and franchised locations had led to a data breach.

... Criminals compromised a third-party POS vendor’s data system and utilized the vendor’s assistance tools to gain remote access—and the ability to deploy malware—to some Huddle House corporate and franchisee POS systems.

... Customers who used a payment card at a Huddle House location between August 1, 2017 and through February 1, 2019 may be at risk. “This date range is based upon our preliminary investigation and we are still conducting our investigation into the scope of this attack,” said Huddle House.
If there is no vendor access, then vendor access cannot be a source of a breach.

Many PCI controls are relevant
• Vendor Password Management [2,8]
• How does a vendor do agent access control? [7]
• Is there always-on access to the store? [12]
Defend Remote Access

Awareness: People
- Physical
- Perimeter Security
- Network Segmentation
- Host and Application
- Critical Assets

People: rules for enabling remote access
- Perimeter Security
  - IDS
  - Ephemeral Connections
- Segmentation
  - Segment away from Cardholder Data
- Application Level
  - Password management
Remote Access Attack Vector

• The PCI DSS offers a great list of controls – implement them!

• Ask your IT department or network vendor
  • Is there an AoC for the support center of vendors accessing critical data?
  • Can vendors access my stores from anywhere at will?
  • Do vendors have permanent or ephemeral remote access to my stores?
  • Can vendors initiate access to the store without our knowledge or permission?
  • Is all access by vendors logged? How do I see the logs?
  • Will vendor access for support self-terminate?
Summary

• Be an onion, not a box of bon-bons!
• Segment!
• Make sure you can visualize EVERYTHING attached to your network
• The PCI DSS is a great source of guidance to add layers of security
• Ask your IT department or vendors specific questions about the presence of controls.