

Secure Configurations for Hardware and Software

Presenter: Ms. Melissa Vice

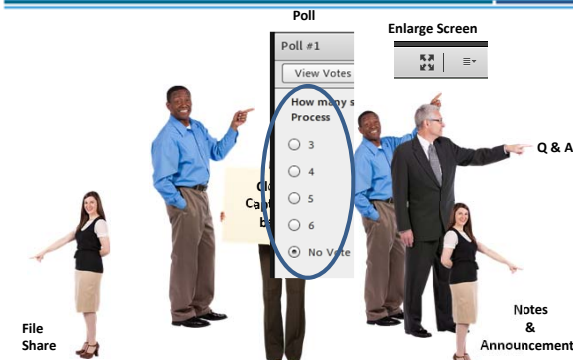



Ms. Vice joined CDSE as an Information Technology Specialist and Courseware Developer in May 2009.

Prior to joining CDSE, Ms. Vice was the Global Database Administrator for commercial and military aircraft engine repairs worldwide at General Electric Aviation Division.

Ms. Vice holds two Associates Degrees (Science of Advertising Design and Computer Information Science), an Undergrad Certificate in Information Assurance, and is wrapping up a dual Bachelors / Masters in Cybersecurity at the University of Maryland. She is the 2010 winner of the University of Maryland's Gordon Prize for Managing Cybersecurity Resources.


Navigating the Meeting Room



The screenshot shows a meeting room interface with several elements:

- Poll #1:** A poll titled "How many s Process" with options 3, 4, 5, 6, and No Vote. The "No Vote" option is selected.
- Enlarge Screen:** A button with a magnifying glass icon.
- Q & A:** A section for questions and answers.
- Notes & Announcements:** A section for notes and announcements.
- File Share:** A section for file sharing.

Center for Development of Security Excellence
CDSE
Learn. Perform. Protect.

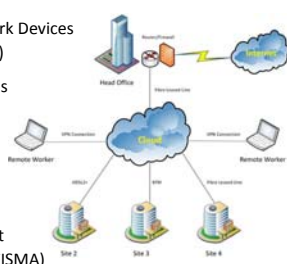


Secure Configurations for Hardware and Software

Secure Configurations for Hardware and Software **CDSE**

Topics:

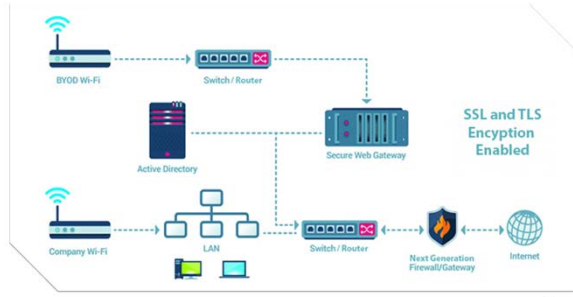
- Cybersecurity Concerns for Network Devices (Routers, Firewalls, and Gateways)
- Hardening Critical Security Controls to Ensure Device Integrity
- Baseline Compliance Reporting
- Automated Software Solutions (features & potential benefits)
- Secure Configuration Management (i.e.: NIST SP800 series, RMF and FISMA)



5

Secure Configurations for Hardware and Software **CDSE**

Cybersecurity Concerns for Network Devices



6

Secure Configurations for Hardware and Software CDSE

Cybersecurity Concerns for Network Devices

BYOD Wi-Fi

Switch / Router

SSL and TLS Encryption Enabled

Company Wi-Fi

LAN

Switch / Router

Next Generation Firewall/Gateway

Internet

7

Secure Configurations for Hardware and Software CDSE

Cybersecurity Concerns for Network Devices

BYOD Wi-Fi

Switch / Router

DO NOT SECURE TRANSACTION

TLS TRANSACTION

Company Wi-Fi

LAN

Switch / Router

Next Generation Firewall/Gateway




Internet

8

Secure Configurations for Hardware and Software CDSE

Polling Question 1:

Does your organization have a policy to use TLS encryption on internal communications?

-  Yes
-  No
-  I really don't know

9

Secure Configurations for Hardware and Software CDSE

The diagram illustrates two network security configurations. The top part, titled "SSL In-Line Inspection Connected to Downstream Tools", shows a Server connected to a Firewall, which is connected to a User's Laptop. An SSL In-Line Inspection Device is positioned between the Server and the Firewall. Data flows from the Server through the inspection device to the Firewall, and then to the User's Laptop. A Forensics Tool and a DLP (Data Loss Prevention) system are also connected to the network path. The bottom part, titled "Internal SSL In-Line Inspection", shows a similar setup but without the Firewall, with the SSL In-Line Inspection Device placed directly between the Server and the User's Laptop.

100% SECURE TRANSACTION
TLS
TRANSACTION

Encryption for 100% of Network Traffic

10

Secure Configurations for Hardware and Software CDSE

Hardening Critical Security Controls

The diagram shows two network scenarios. The top scenario, "BYOD Wi-Fi", features a wireless router connected to a Switch/Router. The bottom scenario, "Company Wi-Fi", shows a wireless router connected to a LAN (Local Area Network) with several devices, which is then connected to a Switch/Router. Both scenarios include a "100% SECURE TRANSACTION TLS TRANSACTION" badge. The Internet is represented by a globe icon on the right.

11

Secure Configurations for Hardware and Software CDSE

Hardening Critical Security Controls

This diagram illustrates a more complex network security architecture. It includes a BYOD Wi-Fi section and a Company Wi-Fi section. The Company Wi-Fi is connected to a LAN with devices, which is then connected to a Switch/Router. This switch/router is connected to an Active Directory server and a Secure Web Gateway. The Secure Web Gateway is connected to a Next Generation Firewall/Gateway, which is finally connected to the Internet. A "100% SECURE TRANSACTION TLS TRANSACTION" badge is present.

12

Secure Configurations for Hardware and Software CDSE

Hardening Critical Security Controls

13

Secure Configurations for Hardware and Software CDSE

Polling Question 2:

Does your network include Next Generation Firewalls (NGFW) and/ or Secure Web Gateway (SWG) devices?

- Yes
- No
- I really don't know

14

Secure Configurations for Hardware and Software CDSE

Baseline Compliance Reporting

PCI – Federally mandated standards regarding credit card handling by financial institutions. PCI Data Security Standard compliance is validated annually.

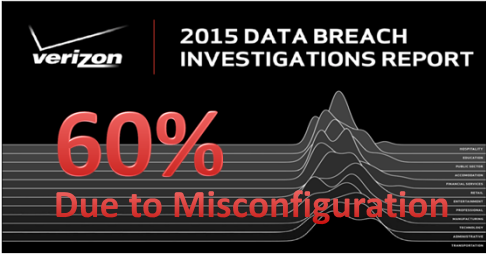
HIPAA – Standards for protecting sensitive patient data and protected health information (PHI) for physical, network and processing security. HIPAA compliance is audited by the U.S. Department of Health & Human Services.

FISMA – The Department of Homeland Security provides operational support for federal agencies in securing their information systems and reporting of compromises.

15

Secure Configurations for Hardware and Software CDSE

Baseline Compliance Reporting



Source: Verizon 2105 Data Breach Investigations Report 16

Secure Configurations for Hardware and Software CDSE

Policy


Develop Baseline Compliance Reporting policies that support your organizational requirements.



Secure Configurations for Hardware and Software CDSE

Organization Policy Safeguards:

- User Privacy
- TLS Certificate Validation
- Enforcement Encryption Standards
- Network and Endpoint Controls



*See www.SANS.org Policy Templates

Secure Configurations for Hardware and Software CDSE

Automated Software Solution

Network Configuration and Change Management (NCCM) – Establishes Configuration Items (CIs) for every networked device to record baseline settings for internal policies and regulatory mandates.



19

Secure Configurations for Hardware and Software CDSE

Automated Software Solution

Don't let system changes take you by surprise.




20

Secure Configurations for Hardware and Software CDSE

Risk Management Framework

RMF – Is a risk-based approach to an organization-wide information and cybersecurity controls.



* See NIST SP 800-37 (www.NIST.gov)

21

Secure Configurations for Hardware and Software CDSE

Risk Management Framework

The 6-Step cycle includes:

- Step 1: Categorize
- Step 2: Select
- Step 3: Implement
- Step 4: Assess
- Step 5: Authorize
- Step 6: Monitor

22

Secure Configurations for Hardware and Software CDSE

Conclusion

Secure Configurations for Hardware and Software CDSE

Conclusion

Secure Configurations for Hardware and Software CDSE


CDSE's website:
<http://www.cdse.edu>



25

Secure Configurations for Hardware and Software CDSE

Questions



26

Secure Configurations for Hardware and Software CDSE

Feedback

Before we conclude today's presentation, we hope you'll take a moment to participate in our feedback questionnaire. Your feedback is very helpful to us and is greatly appreciated. If you have ideas for future webinar topics, you're able to share these in the questionnaire.



 **Secure Configurations for Hardware and Software** 

Cybersecurity Training Products and POC

Past Webinars

- [Information Security Continuous Monitoring](#)
- [Monthly Cyber Awareness](#)
- [Trusted Downloading](#)
- [NISP C&A Process and OBMS](#)

All Other Training

- [CDSE Cybersecurity](#)

Melissa Vice
E-mail:
Melissa.Vice@dss.mil

For More Training Info:
cybersecurity.training@dss.mil

28
