System Security Are We At Risk?

Maria Thompson

State Chief Risk Officer

May 2, 2019

NC DIT

Agenda

- Current State Threat Landscape
- Why is this important to me?
- Top 10 Database Vulnerabilities
- Cyber Best Practices
- Cybersecurity Incident Reporting Requirements
- Questions?

Current State of Cyber Threat Landscape

You are only as strong as the weakest link.

- More than 50 percent of incoming emails are identified as phishing, virus delivery and SPAM.
- This year there have been three reported cyber incidents involving local counties.
- FBI lists NC as the fifth highest state in revenue lost to cybercrime in 2018.
- State agencies are susceptible to phishing emails.
- The use of Internet of Things increase daily … along with their associated risks.
- Business owners continue to accept risks blindly.
- Patch management is NOT where it should be.

Current State of Cyber Threat Landscape

Today's cyber risks are increasing. New technologies bring greater capabilities at a trade off. Convergence of traditional systems and IT networks create more risks.

- Unprotected databases put 65 percent of American households at risk: Goldmine for identity thieves
- Atrium Health, a healthcare and wellness provider serving North Carolina, reveals an intruder had unauthorized access to its databases through a third-party vendor.
- MongoDB databases still being held for ransom, two years after attacks started
- 2020 Census and fears of Database Reconstruction Attacks
- Docker breach of 190,000 users exposes lack of two-factor authentication

Why is this important to me?

As database administrators, you CAN be the weakest link.

Top 10 Database Vulnerabilities

- Deployment failures
- Excessive user privilege
- Poor password management
- Lack of segregation
- Missing patches
- Poor audit trails
- Inadequate database backups
- Unencrypted data
- Database management
- The human factor

Cyber Best Practices

> *"As financially motivated attackers turn their attention 'up the stack' to the application layer, business applications such as ERP, CRM and human resources are attractive targets. In many organizations, the ERP application is maintained by a completely separate team and security has not been a high priority. As a result, systems are often left unpatched for years in the name of operational availability."*

Gartner, Hype Cycle for Application Security, 2017, July 2017 [1]

Cyber Best Practices

- Prioritize critical and high patches for remediation.
- Implement MFA for privilege users.
- Ensure you have adequate logging turned on, and that the logs are sent to a consolidated area for continuous monitoring.
- If the solution is vendor managed, review the following:
  - Vendor's security patching cadence
  - Privileges of users responsible for administration or development activities, as well as those of interconnected systems
  - A repeatable process that ensures that gaps identified within the established security baseline are prevented or detected in a timely manner, and that corrections are implemented
- Subscribe to vendor and open source security feeds to get proactive reporting on threats to your specific systems.
- Share information with your peers: One team, one fight.

Cyber Best Practices

- Effective cybersecurity practices, governance policies and risk assessment methods.
- Cyber Hygiene
  - Change passwords frequently. Hackers use password information leaked in other breaches.
  - Implement strong account management and access control practices.
- Develop, implement and test Incident Response Plans.
- Conduct cyber-resiliency exercises.
  - What happens to your business if this system is not accessible?
  - What is your continuity of operations plan?
- Vendor Risk Management
  - Tailor your audits to meet the specifics of the type of system and threats associated.
  - Ensure vendor stays updated on patch management and product lifecycle.

Free Cybersecurity Training Resources

- Federal Virtual Training Environment (FedVTE)

Course proficiency ranges from beginner to advanced levels. Several courses align with a variety of IT certifications such as Certified Information Systems Security Professional (CISSP), CISA, CEH, Pen Testing etc.

https://niccs.us-cert.gov/training/fedvte

- National Initiative for Cybersecurity Careers and Studies

https//niccs.us-cert.gov/formal-education

Let’s Connect!

@NCDIT
@BroadbandIO
@ncicenter

NCDIT

@NCDIT

NC Department of Information Technology

NC DIT

it.nc.gov