Technology Director Meeting

EDUCATION SERVICE CENTER, REGION 20

Serving the Educational Community

ESC★20
Serving the Educational Community

Mission: ESC-20 positively impacts the learning community **through high quality, cost effective products and services.**

Vision: To be the **definitive choice** for **leadership, innovation,** and the **advancement of learning.**

We believe...

in **service** first • **change is opportunity** • our employees **drive our success** • in **cultivating strengths** **collaboration** maximizes results • **learning** is **life-long** • in **purposeful** and **effective communication**

Strategic Drivers

Customer Service:
Create a service culture through a focus on the total customer experience.

Customer Focus: Listen to our customers, anticipate their needs, and create value that exceeds their expectations.

Employee Talent: Attract, grow, and retain top talent.

Continuous Improvement:
Create a culture of excellence through a mindset of continuous improvement.

Quality Objectives

Positive Impact on Education

Customer Satisfaction

Employee Satisfaction

Operational Excellence

Public Awareness/Relations

Strategies

Build relationships and **engage stakeholders**

Provide comprehensive **school improvement services** and **support**

Recruit and retain **high quality workforce**

Allocate resources to **develop** and sustain **quality products** and **services**

Implement a **performance excellence management system**

Agenda

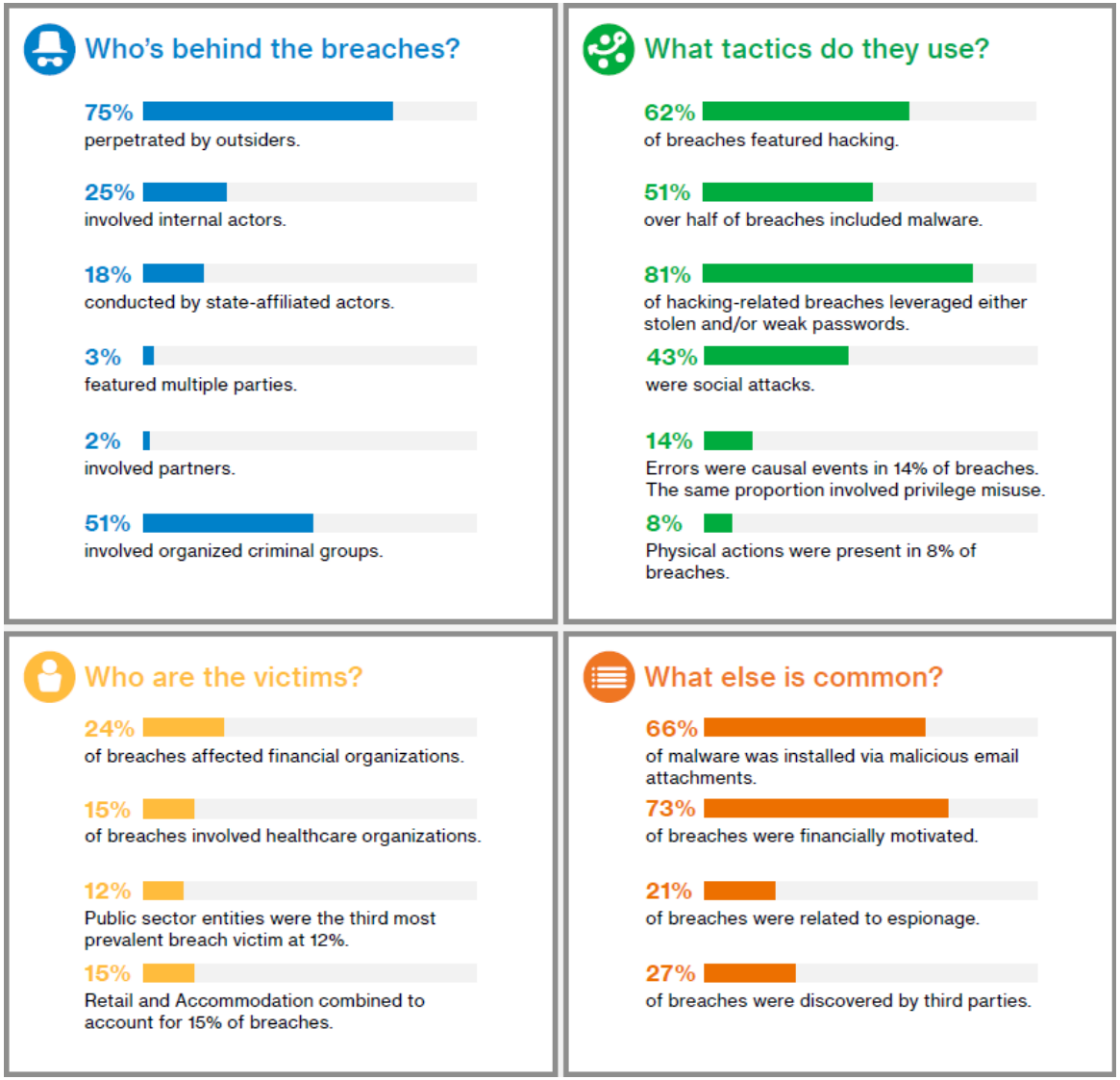
ESC★20
Serving the Educational Community

- 2017 Verizon Data Breach Investigations Report
- Cyber Alerts – Spread the word!
- Network Assessment – What's in it?

Verizon Data Breach Investigation Report

ESC 20 Serving the Educational Community

DBIR Snapshot



Verizon Data Breach Investigation Report

ESC 20 Serving the Educational Community

Cyber Threats to the Education Sector

Cyber-Espionage

Attacks linked to state-affiliated actors, and/or with the motive of espionage.

Welcome to the long game

A malicious email is the cyber spy's favored way in. But this is no smash and grab. The initial email is typically followed by tactics aimed at blending in, giving the attacker time to collect the data that they need.

What you can do

Throw your weight behind security awareness training and encourage your teams to report phishy emails. Make it difficult for the adversary to pivot from a compromised desktop to other devices on your network.

Miscellaneous Errors

Unintentional actions that directly compromised the security of company data.

Mistakes were made

They can appear innocuous, but data lost through errors can be harmful too. Especially if – as in 76% of cases – it's the customer who makes you aware of your slip-up.

What you can do

Have, and enforce, a formal procedure for disposing of anything that might contain sensitive data. And establish a four-eyes policy for publishing information.

Everything Else

Any incident that did not classify as one of the nine patterns.

Beware of imposters

This may be a catch-all category, but that doesn't mean there aren't interesting and important trends. A key emerging tactic is email compromises: where "the CEO" orders wire transfers with an urgent and believable back story.

What you can do

Hammer home to your teams – particularly in finance – that no one will request a payment via unauthorized processes. Also ask IT to mark external emails with an unmistakable stamp.

Cyber Alerts – Spread the Word!

- SANS NewsBites
- Security Tracker Vulnerability Summaries
- US-CERT – Alerts, Bulletins, Tips, Technical Documents
- Department of Homeland Security - Homeland Security Information Network (HSIN)
- National Cybersecurity and Communications Integration Center (NCCIC)
- Multi-State Information Sharing & Analysis Center (MS-ISAC) - Texas

Network Security Assessment – What's in it?

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle"

Sun Tzu - The Art of War

Network Security Assessment – What's in it?

A network consists of the devices that facilitate packet forwarding (routers, switches, and firewalls) and the interconnected devices that process, store, and share data (PCs, servers) as well as the people that operate, manage, and control these devices.

The goal of a network security assessment is to identify network and system vulnerabilities by assessing management, operations, and technical aspects of an information system and provide recommendations to remediate or improve the security posture.

Network Security Assessment – What's in it?

ESC 20 Serving the Educational Community

Ohio Prison Inmates Built Secret Computers and Hid Them in the Ceiling

- Inmates at an Ohio prison managed to build two computers from parts taken from a prison computer skills and recycling program.
- Officials were alerted to the problem when the Ohio Department of Rehabilitation and Correction (ODRC) IT department received an email alerting them that a computer had exceeded its daily Internet use threshold.

Read more in:

- https://arstechnica.com: Inmates built computers hidden in ceiling, connected them to prison network
- http://computerworld.com: Crafty Ohio inmates scavenged parts, built PCs for hacking and hid them in ceiling
- http://watchdog.ohio.gov/Portals/0/pdf/investigations/2015-CA00043.pdf

  Report of Investigation

Network Security Assessment – What's in it?

Recommend a five phase approach to network security assessments:

1) Planning
2) Survey
3) Analysis
4) Reporting
5) Remediation

Conclusion

The network security assessment produces an understanding of the infrastructure and architecture of the network.

The network documentation developed during the survey and analysis is invaluable to the operation and maintenance of the network post assessment.

Vulnerability reports provide prioritized and actionable remediation objectives.

The products delivered from the network assessment could be used as a starting point to re-engineer or modernize the network.

Contact

Mike Garcia
Security Administrator
210-370-5740
mike.Garcia@esc20.net