BooMUG 2023

“Tales From Nightmare On Cyber Street

October 27th 2023

Mirazon®
Providing Vision for Technology Solutions

Agenda

- *Spooky story of a real-world ransomware*
- *Post-crisis analysis*
- *Where that environment could have improved*
- *What you generically need to watch for*

Mirazon®

The Setup

Our story starts on a warm August morning

- Company has a 5 node production ESXi cluster
- Company has a 6 node DR ESXi cluster
- The DR ESXi Cluster is not domain joined.
- All infrastructure passwords are unique, 32 characters and not-re-used.
- Replicas are sent daily to the DR location
- Backups happen to a different physical server and are stored on an iSCSI connected NetApp
- Production servers are partially moved from an AFA NetApp to a Dell PowerStore

Mirazon

Real world Ransomware

Hold on to your butts

- 3:12 AM – Servers go offline
- 6AM – Company realizes servers are offline
- 8AM – Company calls consultants for help
- Consultants validate all but 8 VMs are encrypted at the VMware level
- Network is immediately locked down, nothing in or out
- Consultants validate backup server is encrypted
- Cyber Security Insurance provider called
- Consultants validate DR environment is encrypted
- Cyber insurance company demands no changes to environment

Mirazon®

Real world Ransomware

- Validation that there is no known copy of missing data available
- Forensics company gets involved
- Consultants find that the “surviving” VMs were cluster VMs that were encrypted from within because they had RDM
- Late on Day 1, consultants find automatic snapshots were enabled on SOME SAN volumes
- A test snapshot restore DOES work, but data is non-quiesced.
- Forensics company starts asking for specific logs, still requests nothing is touched

Mirazon®

Real world Ransomware

- Day 2 starts with more requests from the forensics company or encrypted VMDK that have to be manually uploaded
- Forensics company requests their EDR gets installed on every single workstation and server in the environment
- Lawyers and PR firm brought in for dealing with the attackers
- Negotiations start as a stalling tactic
- Consultants and company negotiate with forensics team to free up one ESXi host to attempt some restores from snapshots
- At the end of day 2 permission is given to keep old datastores and 3 esxi hosts, but start rebuilding the remaining one

Mirazon®

Real world Ransomware

- Host rebuilt from scratch on new subnet
- Snapshot restores able to be done for approximately 40% of environment
- One of those is the data warehouse, which is reverse engineered to rebuild production ERP database
- All front-end servers have to be rebuilt
- Cannot rebuild backup server on original hardware because forensics need it

Mirazon®

Real world Ransomware

- Forensics starts to ask pointed questions about users
- Individual user laptops have to be imaged and uploaded
- More VMDK are uploaded
- 2 physical servers have to be imaged and uploaded
- Individual computers once scanned and validated are put in new networks at each site with new explicit firewall rules
- Day 3 the company is allowed to isolate one single ESXi host for forensics and rebuild the others for production rebuilding

Mirazon®

Real world Ransomware

*How the *&()&#%()@&$)*?*

- While rebuilding is happening the ongoing question is HOW? How did they get multiple unique long, complex passwords?
- Where can passwords be stored NOW for safety?
- On Day 3, the forensics company reveals one of the ERP Admins computer had a session hijacked to the password manager
- That one user had been overlooked for forcing the enablement of MFA
- Over 300 passwords now need to be manually changed and updated

Mirazon®

Real world Ransomware

Impact

- Over 1.5 weeks of ERP outage
- Over 2 months until fully recovered
- 2 weeks of around-the clock work
- Full re-architecture of environment to implement internal segmentation
- Secondary password manager to split exposure

Mirazon®

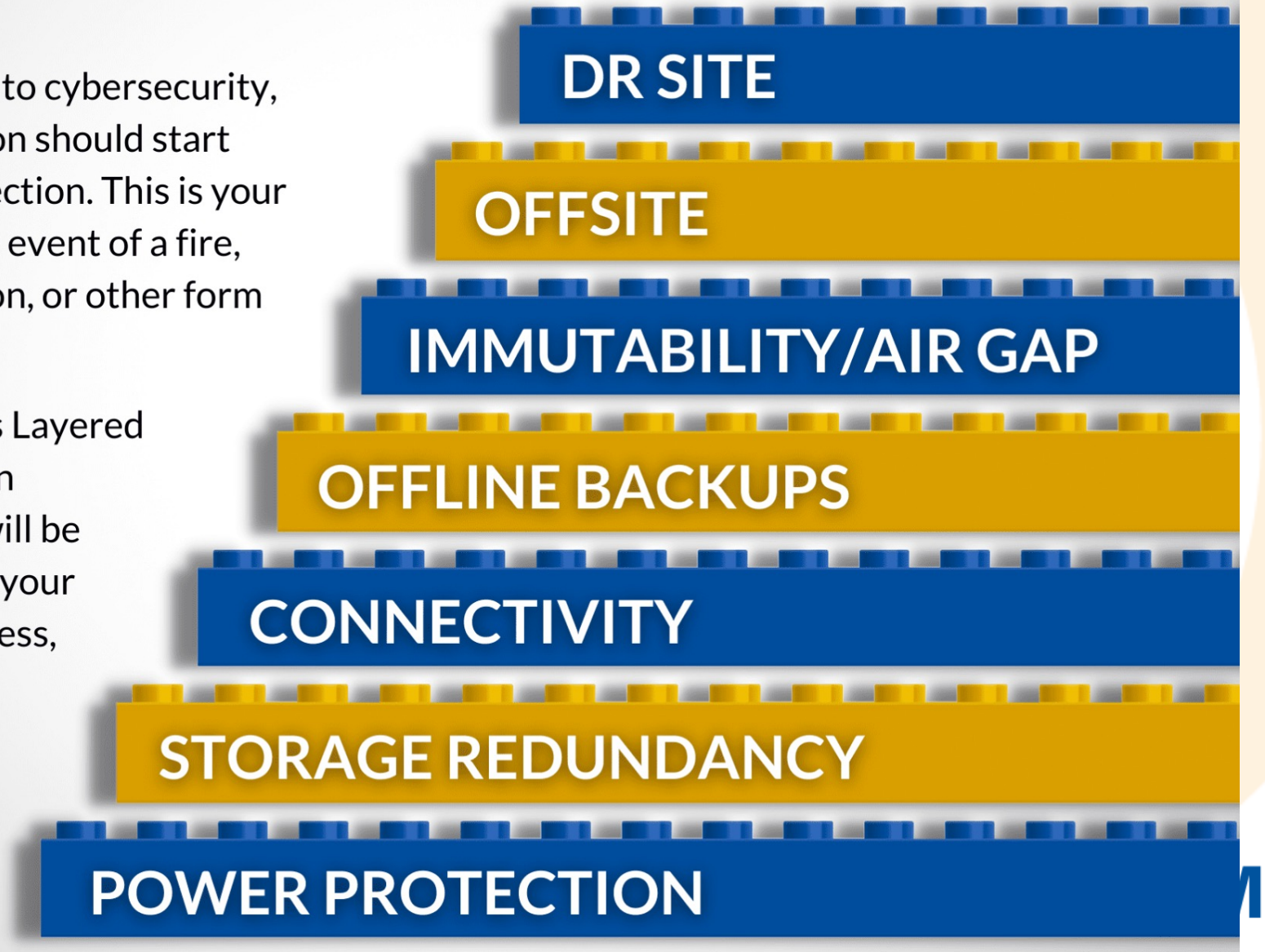
Spooky Background

Mirazon's Layered
Data Protection Strategy

Mirazon
Providing Vision for Technology Solutions

When it comes to cybersecurity, the conversation should start with data protection. This is your backstop in the event of a fire, theft, encryption, or other form of disaster.

With Mirazon's Layered Data Protection Strategy, you will be able to protect your data, and business, on every level.

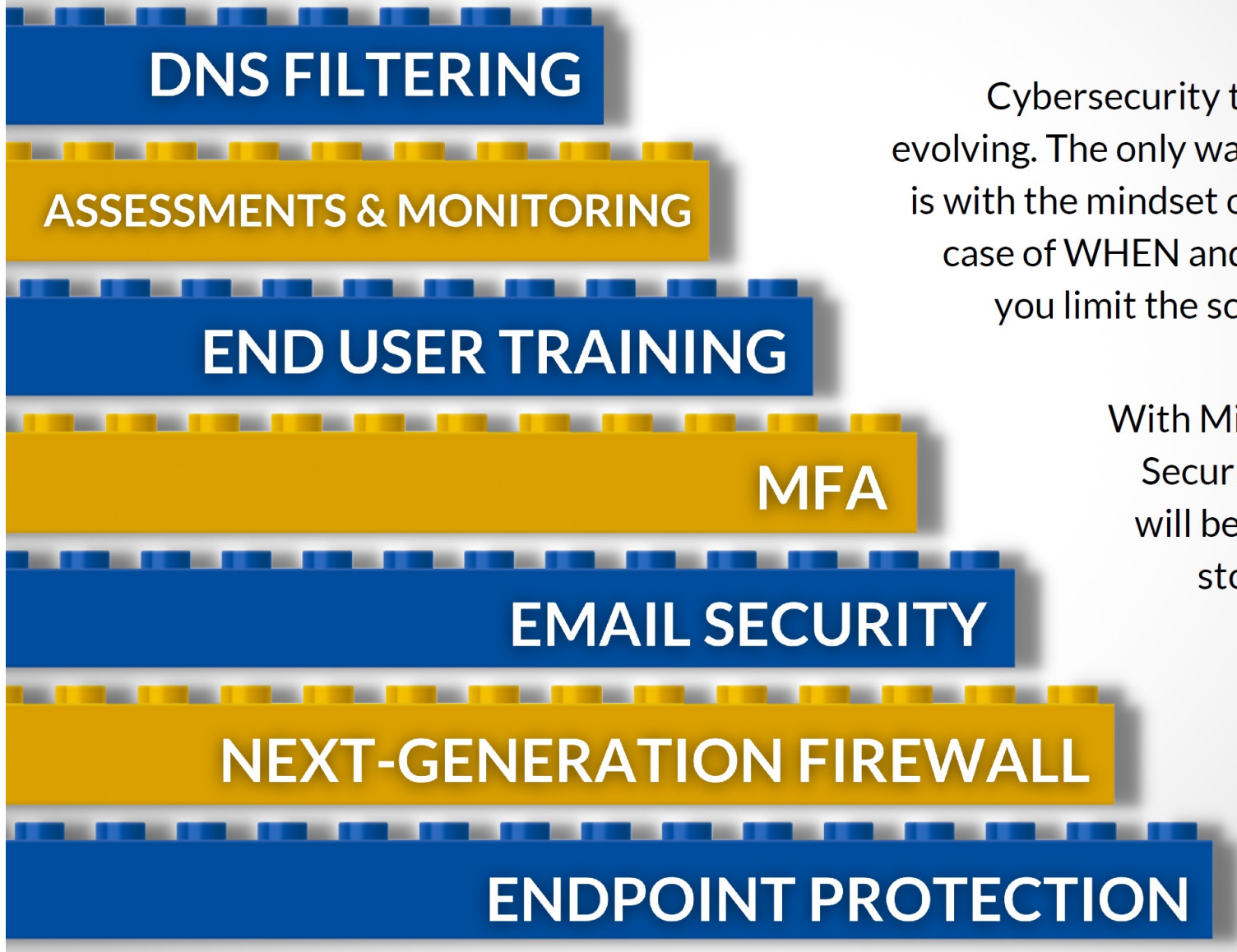


Mirazon.com

Mirazon

Mirazon's Layered Security Strategy

Mirazon®
Providing Vision for Technology Solutions



Cybersecurity threats are ever-evolving. The only way to combat this is with the mindset of assuming it's a case of WHEN and not if -- how do you limit the scale of an attack?

With Mirazon's Layered Security Strategy, you will be able to identify, stop, and minimize cyberattacks.

Mirazon.com

Under Discussed Defensive Measures

Network Segmentation

- Each Deck/Department has a hatch to control what gets in & out (i.e., water, fire, etc.)
- Critical systems, communications, cargo are kept deep within the hull (powder room, CIC, etc.)

Mirazon®

Under Discussed Defensive Measures

Policies, Planning & Education

- A IR/DR plan is only as good as your ability to execute said plan.
- If you are simply “checking a box” you are setting yourself up for failure.
- Plans, backups, etc. should be tested, drilled & reviewed on a regular basis. This can be tests, table top exercises, etc.

Mirazon®

Under Discussed Defensive Measures

Get the most out of what you have.

- Understand the capabilities of what you have & use it to its fullest.
- You don’t need a top end “Zero Trust” solution to NOT make people local admins.
- You don’t need the Gartner Super Magic Hecto-Quadrant email security solution to configure DMARC, DKIM & SPF.

Mirazon®

Under Discussed Defensive Measures

Education: You are the ambassador for IT security

- Security Awareness Training goes beyond a slide deck and phishing tests.
- The business needs to be on board.
- End-users need to feel like they are part of the solution.
- Yeah, it can be frustrating.

Mirazon®

Thanks! Questions?

Scared yet?

Tim Lewis

Brent Earls

Mirazon

Mirazon®

Providing Vision for Technology Solutions

www.mirazon.com