IMAGINE IT

The Q4 2022 State of Cybersecurity

imagineiti.com

The Limitations Of Legacy Cybersecurity Protections

The world has changed, and traditional security technologies like firewalls, antivirus, VPNs, and passwords are no longer enough. Why? Yes, those technologies are still very important, but in every breach you read about, the hacker was able to circumvent them.

How?

- Firewalls sometimes have misconfigurations or are missing critical updates.
- Advanced malware can slip past antivirus software.
- VPN's typically do not have Multi-Factor Authentication (MFA) enforced.
- Users often reuse passwords, and they are prone to providing them to hackers in phishing attacks. And many systems do not have MFA enforced.

Those are just a few of the dozens of ways hackers compromise networks and data. If you are only protecting against 4 of them, and those 4 methods themselves are vulnerable, it's just a matter of time before your org becomes a victim.

What You Can Do To Protect Your Org

Deploy "Modern" Cybersecurity

Modern Cybersecurity meets cyber insurance requirements and significantly reduces the chances of a serious breach. It requires addressing all 5 areas of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (Identify, Protect, Detect, Respond, and Recover).

Let's break this down into digestible pieces...

IDENTIFY

- Document the current gaps via an assessment.
- Establish a Vulnerability Management process to continually discover and remediate issues.
- Annually reassess against the current threat landscape.

PROTECT

- Not all antivirus software is equal. Modern protection requires what is referred to as "Next-Gen" antivirus, which can block more advanced threats.
- Enable MFA on remote access (including VPN), every cloud application, and email.
- Subscribe to additional email protections that scan links and attachments (not just SPAM filtering).

- Enroll users in a Security Awareness program that contains phishing campaigns and training videos.
- Lock down and improve hygiene of the network, Active Directory, and Azure Active Directory / 365 to avoid privilege escalation and lateral spread.

DETECT

- Deploy Threat Hunting technologies (preferably human-led 24/7) to detect attacks that may have bypassed legacy protections.
- Deploy Intrusion Detection technologies on the network, 365, and the Dark Web. Again, to detect attacks that may have bypassed legacy protections.

RESPOND

- Create an Incident Response Plan (IRP). Your IT Managed Service Provider (MSP) should have one.
- Annually rehearse the IRP with your MSP so you can kick out intruders before they complete their objective.

RECOVER

- Upgrade to "immutable" backup systems to avoid hacker destruction. This requires that backups to be segmented (usually via the cloud) and utilize entirely separate credentials and MFA.
- Enroll in a real Cyber Insurance policy (not just a rider). The stronger your security posture the lower your premium will be.

Next step, engage with your MSP.

What's Around The Corner?

Continuous Vulnerability Scanning

Hackers exploit vulnerabilities in networks and the cloud, and once inside can easily elevate privileges and spread laterally. Each org has a significant number of devices and applications, all needing to be securely configured and frequently updated. This requires regular scans and remediation and goes beyond 3rd party assessments due to the depth of the remediation process. This should include:

- Asset discovery and tracking
- External / Internal / Website / 365
- Systems misconfiguration discovery:
    - o Windows / Mac / Linux
    - o Active Directory
    - o Azure Active Directory
    - o Intune / Endpoint Manager
    - o Server File Shares

- Microsoft Secure Score
- Patch compliance
- Application encryption / SSL / TLS compliance

There are solutions that will “continually” scan and discover vulnerabilities. This is desirable as the hackers frequently find new ways to exploit them.

Peter’s Insight

Continually remediating these vulnerabilities will not only block many intruders, but if a hacker succeeds in breaching the system, a hardened network will keep the attacker from elevating privileges and spreading laterally to complete their objective.

Security pro-tip of the quarter

QR Code Security (or lack thereof)

In case you do not know what a QR Code is, it is a square-shaped graphic designed to be scanned by your cell phone, that contains embedded information, typically about a business. You might come across one on a business card, or one that has a restaurant menu embedded, or possibly one in a paid parking lot.

What’s the risk? Think about website URL’s. A URL contains recognizable strings of text that the visitor can review to determine if legit. QR Codes are entirely ineligible, and therefore it is impossible to know if one is legit. What if a bad actor pastes a malicious one over a legit one? How will you know?

If you scan a malicious QR Code with your phone, you can become infected with malware that can spread to other systems.

My advice… never scan a QR Code that is posted in an insecure or public area. And scanning QR Codes posted on websites or email is risky.

Conclusion

Upgrade to “Modern” cybersecurity to protect against modern threats. The old standbys are no longer enough.