IMAGINE IT

The Q1 2022 State of Cybersecurity

imagineiti.com

Cybersecurity insurance now dictates minimum security posture

Back in my Q2 2021 report, I touted the importance of enrolling in a cyber insurance policy. Without it, your entire business is at risk.

Previous to 2021, the cyber insurance questionnaires were fairly basic...

- Do users have Passwords?
- Does your org have a Firewall and Antivirus?
- Is a VPN utilized?
- ...and not much else.

These questions were asking about decades old security practices, and NOT taking into consideration modern threats.

In 2020 and 2021 the cyber insurance companies got hammered with breach and ransomware claims and have learned their lesson. For an org to obtain affordable cyber insurance, an org is now required to attest to 25-30 stringent standards. For example...

- Does your org utilize Next-Generation Antivirus with EDR?
- Does your org subscribe to Defender for 365 (scans links and attachments for malware)?
- Do ALL externally accessible or cloud-based applications require Multi-Factor Authentication (MFA)?
- Is the backup system managed separately from Windows Active Directory? And does it require MFA to administer?
- Is there a documented and recently tested Incident Response Plan?
- ...and many more.

Bottom line, traditional security protections are no match for modern threats. To pass a cyber insurance assessment will require enrollment in a modern Managed Security Program that ticks all the boxes.

What you can do to protect your org

A common risk to businesses is the accidental or intentional leakage of confidential data by its users. For example...

- A disgruntled employee uploads confidential data to a personal email.
- An employee accidentally sends confidential data to an impersonator.

How can an org leverage technology to protect against this? In the Microsoft 365 platform, the solution is called Data Loss Prevention (DLP). Here is how DLP works...

- DLP restricts the accidental or intentional leakage of confidential data, and is enforced via policies that restrict files or data from being sent, moved, copied, shared, printed, etc...
- Policies can be created to alert on, or block desired text strings, like Social Security numbers, credit card numbers, account numbers, PII/PHI - just about anything that has a consistent pattern.
- Alerts are sent to a "compliance team", who then APPROVE or DENY the request before the data is sent.
- Manual searches can be performed to identify non-compliant data within your systems.

Enforcing these policies will significantly reduce the risk of confidential data leakage.

What's Around The Corner?

One of the easiest ways for a hacker to laterally spread across a network is to attack the weaknesses of Windows Active Directory (AD). AD is the platform Microsoft developed over 30 years ago to centrally administer users and devices, and at least 90% of businesses with more than 10 users run AD. However, AD is very old and was not designed with modern threats in mind.

For example, a hacker who initially breaches a basic AD user, within a short period of time can elevate privileges to "Domain Admin", which allows the hacker to take over the network and access most data. This is a huge problem and is one of the root causes of most major breaches you hear about.

The good news is that there is an alternative to Windows Active Directory. Over the past few years Microsoft has created two modern cloud-based and "secure-by-design" user and device management platforms...

- Azure Active Directory (AAD): this is where users are managed, and where it is defined who has access to what. MFA is enforced here, as is Single-Sign On (SSO).
- Intune: is a set of device policies that allow an administrator to enforce policies like passwords, encryption, screen-lock, and hundreds more.

AAD + Intune, by design is much more secure, and significantly reduces the risk of lateral spread and account elevation. Therefore, a small breach is much less likely to become a large breach.

Peter's Insight

Solving this problem starts by adding to the technology planning roadmap a transition from Windows AD to AAD + Intune. The first step is to verify that there are no application compatibility issues.

Security pro-tip of the quarter

Inbound Phone Call Best Practices

While most breaches originate via email, many attackers are now taking to phone scams to bypass email security measures. Here are some user best practices...

- Most agencies and banks will never call; they send notices via postal mail. IT staff will not call unless you first initiate a service request.
- Be suspicious of...
    - ▸ Unsolicited calls from a government agency or big company.
    - ▸ Threats of harm if you do not provide personal or financial info.
    - ▸ Offers that sound to good to be true.
- Do NOT answer calls from unrecognized numbers.
- Do NOT provide sensitive data to callers.
- Do NOT provide Multi-Factor Authentication (MFA) codes to ANY caller – ever!
- Do NOT "press 1 to get off the call list". This flags the spammer that you are real, and you will get MORE spam calls.

Users need to be constantly reminded of these best practices via an online Security Awareness Training system.

Conclusion

Be prepared for a tough cyber insurance assessment next renewal, and therefore, be prepared to quickly remediate the gaps.