PCR
BUSINESS
SYSTEMS

10 ADVANCED CYBERSECURITY CONTROLS YOUR BUSINESS MUST HAVE IN PLACE

Due to the dramatic increase in cybersecurity breaches, we recommend that every business have the following controls in place to protect themselves against a breach.

1 ZERO TRUST APPLICATION CONTROL

Allows user to escalate privileges for approved applications & updates and prevents:

- Applications and updates from running if not approved
- Application access to areas of computing that are not needed
- Common attack tools from running (PowerShell)

Attacks Prevented: Supply chain compromise (Solarwinds & Kaseya), lateral movement once attacker has breached the perimeter

2 MANAGED DETECTION & RESPONSE SOFTWARE

Managed Detection & Response Software monitors systems to detect techniques attackers use to move around the network and deploy a malicious payload once they have breached the perimeter. It is monitored 24/7/365 by a Security Operations Center. Security experts will escalate any items of concern for investigation.

Attacks Prevented: Ransomware, lateral movement once attacker has breached the perimeter, data theft

3 MULTIFACTOR AUTHENTICATION

Email, Vpn, all Internet Facing Logins including SaaS Applications
We can't stress this enough, Multifactor Authentication is the most important control to implement. Each year we see hundreds of thousands of dollars lost from attacks that MFA would eliminate.

Attacks Prevented: Business Email Compromise, Account Compromise, Ransomware, Wire fraud, account change fraud, payables fraud, blackmail

4 MANAGED ANTIVIRUS WITH 24/7/365 SOC MONITORING & THREAT HUNTING

Security experts monitor antivirus and activity on end points. The Security Operations Center monitors hundreds of thousands of endpoints allowing them insight on real attacks as they happen. The intelligence gathered allows the escalation of items that need investigated to local IT. Security experts assist with investigation and escalation to incidence response if needed.

Attacks Prevented: lateral movement once attacker has breached the perimeter, Ransomware, malware activity (key logging, etc.), monitors for common attack methods (PowerShell, escalation of privileges, etc.)

5 INTERNAL & EXTERNAL VULNERABILITY SCANNING

Attackers are running external vulnerability scans on your network. If you routinely do the same you can patch weaknesses that will be used against you. Internal scans will allow you to patch issues that could be used to escalate an attacker once the perimeter is breached.

Attacks Prevented: Ransomware, network perimeter breach, lateral movement once attacker has breached the perimeter

6 INCIDENT RESPONSE PLAN

Attacks are going to happen. Planning what you will do when an attack occurs can be the difference between little to no impact vs. going out of business. Example: Engaging your cyber insurance policy may require forensics. They will want your systems to remain unchanged until the forensics is done, which could take weeks. What is the plan if you can't use any of your current equipment for weeks?

Attacks Prevented: Business Interruption, loss of revenue and employee productivity

7 SECURITY AWARENESS TRAINING

Dark Web Monitoring and Automated Phishing Simulations
Mistakes by end users have the highest probability of leading to a security breach. Training them on the most common scams drastically lowers the chance of mistakes. Continual testing with phishing simulations develops a culture of thinking and analysis of emails before clicking.

Attacks Prevented: Business Email Compromise, Account Compromise, Ransomware

8 SYSTEM PATCHING

Firewall, Servers, Workstation (Microsoft & 3rd Party Apps)
Vendors are constantly releasing updates to patch vulnerabilities in their software. It is critical to have a monthly routine to test, deploy and verify patching. Patching systems should also have the ability to respond to zero day threats and deploy out-of-bounds patches quickly.

Attacks Prevented: Ransomware, network perimeter breach, lateral movement once attacker has breached the perimeter

9 BACKUP & DISASTER RECOVERY PLAN

BDR planning is essential to ensure you can recover from system failure, accidental deletion, malicious staff activity and ransomware. Annual testing and separation from production network are critical (Assume attacker has your admin credentials. If they can get to and delete backups there is a problem).

Attacks Prevented: Ransomware, System Failure, Malicious staff activity, accidental deletion, fire, theft, flood

10 WEB SECURITY MONITORING

Monitor websites for malicious activity and will alert you to any issues before your clients/prospects get infected.

Attacks Prevented: Ruined reputation, liability for damage to 3rd party system activity

PCR BUSINESS SYSTEMS IS SOC 2, TYPE II COMPLIANT

The SOC 2, Type II Report validates that we are qualified, professional, and follow the best practices in the IT industry. This certification was provided by an independent third-party who took an in-depth look into the security controls we have in place. Their report concluded that we are a reliable, safe, and compliant IT Provider.