CROWDSTRIKE

CYBERSECURITY PERSCRIPTION FOR HEALTHCARE ORGANIZATIONS

CROWDSTRIKE® OFFERS THE FOLLOWING INFORMATION AND RECOMMENDATIONS TO HELP IMPROVE YOUR SECURITY POSTURE AND STOP THE BREACH!

EFFECTIVE CYBERSECURITY IS CRITICAL FOR HEALTHCARE

In the event of a breach, healthcare providers can face serious challenges, including disruption of patient care, potential lawsuits and reputational damage. It's no secret that the healthcare industry is under increasing pressure from attackers and auditors alike to modernize its security. With an abundance of high-value, confidential data, often combined with a fragmented infrastructure, it's no wonder healthcare organizations are increasingly in the crosshairs of criminal hackers.

HEALTHCARE IS A HIGH-VALUE TARGET FOR CYBERCRIMINALS

Today, the healthcare industry is the second most targeted vertical in the world. Despite increased regulatory oversight, cyberthreat awareness and security investments, breaches continue to happen. Healthcare organizations are mandated to protect highly sensitive personal health information (PHI) and electronic health records (EHR) that must be accessed quickly. This is exacerbated when information is required to be spread across a variety of endpoints operating on disparate, often outdated operating systems.

RECOMMENDATIONS FOR CLOSING SECURITY GAPS

While it's great to be aware of and understand your security strengths, it's even more important to recognize the gaps in your security so you can bolster your defense against attacks and protect your valuable patient records, employee information and intellectual property.

The following are recommendations that can help increase your current endpoint protection strategy and defend your organization against even the most sophisticated attacks.

Establish and Enforce Security Controls: Security policies are critical when it comes to ensuring the safety, security and well-being of your organization and its patients. Having written, enforced security policies in place is the first step toward establishing an effective security strategy for your organization.

Assign Information Security Roles for Your IT Staff: While the number of people dedicated to security can vary depending on the size of your organization and the scale and complexity of its IT infrastructure, it is vital that responsibility for information security be clearly assigned. This may involve an additional duty for a person who has other IT responsibilities, or it may be a staff of dozens of people, but security responsibility should never be unclear or assumed.

Educate Employees on Security Best Practices: Establishing security controls and then ensuring employees adhere to them are critically important given the sophistication of today's threat actors. Unfortunately, often humans can be the weakest links in an organization's security chain. Periodic security best practices education should be mandatory and can be an efficient, effective way to ensure your employees are complying with your security policies and keeping up to date in helping to maintain your organization's security.

Establish a Mature Security Framework: Proactively managing your organization's cybersecurity maturity is essential for defending against targeted cyberattacks. Unfortunately, targeted attacks no longer require expensive preparatory measures — open source software such as Metasploit can be used to penetrate your organization without writing a file to disk, thus evading traditional signature-based or machine-learning enabled malware prevention. Establishing a set of mature, robust security controls and understanding that prevention alone is not enough, can help you prepare proactively and enable your organization to successfully deal with the next security event.

Be Diligent in Patching Systems and Applications: Today, some of the most common security gaps on endpoints occur from unpatched software — a problem that affects 75 percent of organizations. Patching operating systems and third-party applications is one of the most inexpensive and effective ways to harden your endpoints. It's crucial for your organization to establish a strong patch management process that can ensure critical security patches are installed as soon as possible.

Actively Monitor Endpoints: Simply put, you can't protect what you can't see. Often, network monitoring solutions claim to offer comprehensive coverage of endpoint activity, but they fail to do so. In order to effectively address endpoint monitoring shortcomings, an endpoint detection and response (EDR) solution should be deployed. The right EDR can deliver immediate visibility across all endpoints to let you see what's occurring. By actively monitoring traffic that travels from your hosts, you have complete visibility and context, giving you the actionable information needed to remediate quickly and effectively.

Maintain and Test Your Backups: Healthcare organizations continue to be plagued by ransomware, which now accounts for over 70 percent of malware incidents hitting healthcare in 2017. These attacks encrypt files and delete backups, costing healthcare organizations millions and even impacting patient care by encrypting or destroying patient records. In light of these statistics, healthcare IT and security professionals need to adopt and enforce the "backup rule of three." It is a rule of thumb that requires maintaining three copies of all important data in at least two different formats that includes an off-site backup. In addition, these backups should be routinely tested. Three is the preferred number because, while you might think that keeping even more copies is advantageous, storing that much data can become costly and difficult to manage.

Ensure Comprehensive Endpoint Protection: A simple truth in security is that prevention is not enough. The claims that an antivirus solution will block 99.9 percent of threats, still means a 100 percent probability that one will get through. Once your defenses are penetrated without detection, "silent failure" sets in as attackers move about your network unseen. Healthcare organizations can be vulnerable when attackers circumvent stringent prevention policies. EDR solutions that provide continuous endpoint visibility are able to identify and record security events so that fast response and remediation are possible. You should also augment endpoint protection by integrating proactive managed threat hunting to detect emerging and advanced threats.

Attain Real-Time and Historical Visibility: Visibility is not just about seeing your endpoints in real time, but also gaining historical insight and adding context to events that have occurred. EDR is recommended because it can bring immediate visibility to what is happening on an endpoint, allowing security teams to accelerate their ability to respond and act.

Establish Incident Response Plans: Just as people inoculate themselves for flu season and take daily multi-vitamins, regularly reviewing your incident response plans are critical, and CrowdStrike recommends that this include taking active steps to prepare for a breach. Having a well-thought-out incident response plan will help you identify and eliminate active intruders, understand the vulnerabilities that enabled them to gain access, and show you how to restore the confidentiality, integrity and availability of your data and systems.

Augment Security with Threat Intelligence: Having the right technology, tools, and people is not enough to stay ahead of a determined attacker. You need information that can show you who is targeting you and what vectors they may take to infiltrate your organization. Threat intelligence offers security teams substantial advantages, providing the information needed to optimize prevention, detection and response, while keeping your security team a step ahead of adversaries.

Know the Threats Targeting Your Organization: Insider threats comprise 68 percent of the threats healthcare organizations face. In addition, after financial institutions, healthcare is the industry most targeted by nation-state and eCrime adversaries. Choosing a solution that can address the advanced tools, techniques and procedures (TTPs) of well-funded, sophisticated adversaries, while simultaneously stopping insider threats is critical to protecting your organization's endpoints. Insider threats have become prevalent with employee misuse of resources a common occurrence. To increase security, it is recommended that in addition to consolidating data egress points, organizations need to remind employees periodically of organizational policies and procedures to help maintain accountability.

ABOUT CROWDSTRIKE

CrowdStrike® is the leader in cloud-delivered endpoint protection. The CrowdStrike Falcon® platform offers instant visibility and protection across the enterprise and prevents attacks on endpoints on or off the network. Falcon seamlessly unifies next-generation AV with best-in-class endpoint detection and response, backed by 24/7 managed hunting. There's much more to the story of how Falcon has redefined endpoint protection but there's only one thing to remember about CrowdStrike: We stop breaches.

To learn more, visit: https://www.crowdstrike.com/solutions/protecting-healthcare-organizations/

For questions, contact: healthcare@crowdstrike.com