October 29, 2018

It's time to talk about your CYBER audit policy

CYBERSECURITY
BY DAVID MURPHY

Imagine for a moment that your organization is hit with a malicious Trojan that your office’s Information Technology (IT) staff hasn’t noticed for months, and it maintained persistence on one of your file servers where your team maintains sensitive documentation. Obviously, your first goal is execution of your well-documented incident response plan. (You do have one of those prepared, don’t you?) So, you work on containment and eradication of the malware, and then comes the second question that should logically follow an intrusion of this types. Did they take any of the sensitive data stored on this server?

Your ability to respond to an incident and answer questions like the one mentioned previously will rely on your skill to have the right personnel trained in incident response or calling in a team that can help answer those questions and having sound group audit policies in place for the servers affected. There have been many incidents I have personally responded to where we could have answered more questions about the details surrounding the intrusion, but lack of audit policy and proper backups of the logs prevents a detailed picture of what happened. Forensic examinations of the hard drives are all that is left in those cases, and that unfortunately, can cost precious time to get that peace of mind you would like to have.

If you’re currently asking yourself what you should do to get up to speed on this, the answers for a sound audit policy start with matching standards developed by organizations who have already studied what audit policies are necessary. Center for Internet Security (CIS) benchmarks are the place to start, but you should consider additional items to audit if it is a very sensitive system. Strong audit policies are also a great place to help discover malware beyond just the initial infection. Consider the installation of a Security Information and Event Management (SIEM) tool if possible. SIEM software is going to assist in efforts to discover the lateral movement of malware and command and control (C2) connections or exfiltration. You can also perform advanced data analytics and stop threats before they become a much larger problem.

In today’s ever-increasing threat landscape, your cybersecurity practices need to be at the top of their game. Don’t just rely on the anti-virus software installed on systems. With the advent of the cloud integration, anti-virus companies are getting better at detecting and handling threats, but they still miss a lot of threats, and it shouldn’t be something to rely on totally for your overall security posture. A lot of firewalls these days also come with built-in Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS). Ensure you have a team taking the time to look through events generated by these devices because these will only alert you and maybe block the communication, but these devices don’t perform remediation of the affected systems.

Cybersecurity development of any organization should be as important as locking your doors at night. Set your security and audit controls up and test them frequently, so you are prepared to handle to the worst of scenarios. Your organization should consider IT audits and penetration tests or purple team exercises as part of your continued effort to secure the network. We also recommend that you keep backups prepared in case of a catastrophic event.

You've heard our thoughts... We'd like to hear yours

The Schneider Downs Our Thoughts On blog exists to create a dialogue on issues that are important to organizations and individuals. While we enjoy sharing our ideas and insights, we're especially interested in what you may have to say. If you have a question or a comment about this article – or any article from the Our Thoughts On blog – we hope you'll share it with us. After all, a dialogue is an exchange of ideas, and we'd like to hear from you. Email us at contactSD@schneiderdowns.com.

Material discussed is meant for informational purposes only, and it is not to be construed as investment, tax, or legal advice. Please note that individual situations can vary. Therefore, this information should be relied upon when coordinated with individual professional advice.