INFORMATION TECHNOLOGY UPDATE

Keeping Up with the Joneses – Incident Response Planning

Hackers work around the clock, and most company-employed security personnel work eight hours a day. Even those companies that have several shifts to provide 24/7 monitoring would still admit there are gaps in what can be looked at and reviewed. A typical port scanner will send roughly 500 packets per second at a target from which it is trying to get information. However, good hackers know how to slow down the port scans. Therefore, even a company with above-average network monitoring does not have the resources to investigate every IP address that hits its firewall. This makes it difficult to "keep up with the Joneses."

Because it's getting so difficult to get ahead of the hackers, most security experts will tell you that today, it's not a matter of ***if*** you will be breached, it's a matter of ***when*** you will be breached. In fact, security experts say that for certain externally facing systems such as email and web servers, you should assume they have already been breached and use caution when posting data or sending emails to/through these systems. As a best practice, it's safer to send sensitive information through secure email.

While the above is a scary thought, it proves one thing: Incident response planning must be a paramount portion of any information technology and information security environment. If you assume you will be attacked and/or breached, how quickly can you detect this attack or breach and how quickly can you isolate and stop the attack or breach takes priority in securing your networks.

A good incident response plan should detail monitoring procedures of the firewall, network, and applications. This portion of the plan should include the type and frequency of monitoring and the individual performing it. Second, an incident response plan should outline what will be done for each type of potential attack/breach. For attacks, a decision tree detailing what will be done for the different types of potential attacks should be devised. In other words, does the institution investigate all types of attacks (even down to port scans that can be happening hourly) or are only certain types of activities monitored? Are all IP addresses of potential attacks blocked or only ones that have reached a certain risk threshold? Describing how an attack can be blocked or a breach can be contained once detected should serve as the main focus of this plan. If an actual breach is detected, what forensic information will be gathered and retained? Who will notify the press, regulators, and other staff members is another important portion of the plan.

While there's a significance in having an incident response plan, being able to test its functionality is key. One of the best times to test an incident response plan is during an annual attack and penetration test, mainly if the testing is covering both an internal and external perspective. If your IT department can detect internal and external traffic from the tester,

2009 Mackenzie Way, Suite 340 Cranberry Twp., PA 16066 | Phone (724) 934-0344 | Fax (724) 934-0345 | Email: info@srsnodgrass.com
1275 Glenlivet Drive, Suite 135 Allentown, PA 18106 | Phone (610) 530-8885 | Fax (610) 530-0409
2100 Renaissance Blvd., Suite 110 King of Prussia, PA 19406 | Phone (610) 278-9800

you'll know how it stands up against an attack. If this test was a real threat to the company, what actions would have been taken? Perhaps in the early part of the testing, you would have your IT staff take those actions and then later permit the traffic through to allow for a more detailed report. If any gaps in your plan are found, you can make adjustments to ensure you are able to respond faster and more appropriately for future tests or attacks.

While IT personnel may never "get ahead" of hackers and know all of their tricks, detecting their attacks and breaches in a timely manner is the solution to ensuring that anticipated attacks and breaches result in minimal data loss and cause the least amount of harm to your organization.

QUESTIONS?

If you have any questions regarding this Update, please feel free to contact Jeremy Burris, Rob Haller, or Chris Kreutzer at (724) 934-0344 or (800) 580-7738, or email **jburris@srsnodgrass.com**, **rhaller@srsnodgrass.com**, or **ckreutzer@srsnodgrass.com**.