Intrusion Prevention "Hand-in-Hand" Services

Intrusion Prevention

You are currently protecting your Information System and data from unauthorized access by utilizing an Intrusion Prevention System. We're there 24x7x365, watching your network and RESPONDING to threats. You are complying with regulations and best practices. What else can you do?

Hand-in-Hand Services

Many examiners are starting to ask our clients about additional safeguards related to log monitoring, web defacement, and phishing response. Our Intrusion Prevention System can be leveraged to offer a wide range of additional services that can help our clients respond to current examiner focus. As such we have created a set of "hand-in-hand services."

Log Monitoring

Our existing sensors can be used to collect, consolidate, and monitor your security logs -

- Logs will be consolidated and archived outside of your systems;
- Database is human and computer analyzed in real time;
- Alerts are sent via e-mail or by phone as per your Decision Tree (extended from the initial IPS setup);
- Daily summary reports;
- Web Interface for live and long term reporting;
- Audits and examinations will show that appropriate logging controls are in place;
- Your staff will be much more productive.

Financial institutions should take reasonable steps to ensure that sufficient data is collected from secure log files to identify and respond to security incidents and to monitor and enforce policy compliance.

Appropriate logging controls ensure that security personnel can review and analyze log data to identify unauthorized access attempts and security violations, provide support for personnel actions, and aid in reconstructing compromised systems.

-FFIEC Information Security Booklet

One of the most dramatic findings from this year's survey is the exponential increase in website incidents.

- CSI/FBI Computer Crime and Security

Web Defacement Monitoring

Unlike other attack cases where the hacker hides his activities, in web defacement incidents, the major goal of the hacker is to gain publicity by demonstrating the weakness of the existing security measures. This can be done by inserting or substituting defamatory or otherwise damaging information into the website. The defacement of an organization's website exposes visitors to misleading information until the unauthorized change is discovered and corrected. This leads to strategic, reputational, operational, security and legal risk. Impact severity is very high.

Our Web Defacement Monitoring service allows our team of security professionals to "crawl" and scan your website line by line many times per day. When a change is made, it generates an alert. Our NOC reviews the web page to determine if the change would be deemed authorized or acceptable. If the change is determined to be a defacement situation, our staff can quickly notify you and can provide the last known good code immediately, depending on the current methodology documented in the Decision Tree. Forensics are not included in the service.

Phishing Response

Phishing is becoming a large problem for smaller institutions. Most of our clients have decided that the expensive phishing detection services currently available do not warrant the investment, and we agree. But there are a number of things you can do and have prepared to not only help prevent, but to detect and respond to a phishing incident. We can help you ensure your Incident Response Decision Tree is properly tooled for phishing response. Our affiliations with law enforcement, primarily because of our founding and sponsorship of bleedingsnort, allows us to take down phishing sites quickly.