From: Greyhat [mailto:greyhat@greyhat.com]
Sent: Tuesday, April 09, 2013 02:36 AM
To: cyberframework
Cc: Sedgewick, Adam
Subject: Developing a Framework to Improve Critical Infrastructure Cybersecurity

Please disregard the previous submission and accept this version in its place.

GRAYHAT

Current Risk Management Practices

NIST solicits information about how organizations assess risk; how cybersecurity factors into that risk assessment; the current usage of existing cybersecurity frameworks, standards, and guidelines; and other management practices related to cybersecurity. In addition, NIST is interested in understanding whether particular frameworks, standards, guidelines, and/or best practices are mandated by legal or regulatory requirements and the challenges organizations perceive in meeting such requirements. This will assist in NIST's goal of developing a Framework that includes and identifies common practices across sectors.

1. What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?

GRAYHAT RESPONSE

For the past 20 years, we have relied on firewalls, antivirus, and patching to be the foundation for security for enterprise and consumer systems from notebooks, tablets, and desktops to servers.

The primary focus has been on the Microsoft Windows platform because this single platform is the most connected on the Internet.
Reference: http://en.wikipedia.org/wiki/Usage_share_of_operating_systems

Since 2002 and the Bill Gates' Trustworthy Computing memo to all Microsoft employees, Microsoft has instituted many internal and external security programs to raise the level of security at Microsoft.
Reference: http://www.wired.com/techbiz/media/news/2002/01/49826

Other vendors should follow suit. Microsoft?s security turn around should be emulated.

In the past few years, several factors have destabilized the security of the Internet and its associated ecosystem:
- Mobile operating systems have been multiplying in the Internet of things with Apple iOS and Android as the new dominant operating systems connecting to the Internet.
Reference: http://en.wikipedia.org/wiki/Usage_share_of_operating_systems
- Antivirus no longer is sufficient against the malware threat that is associated with phishing, spear phishing, 0-day attacks, and other targeted attacks and also drive-by malware loaded on prominent websites.

With the diminished effectiveness of antivirus, companies now need to rely on the following to have a fighting chance to deal with the threats listed above:
A- System hardening.
B- Hardened broswers
C- Disabling of features in the browser or macros in Microsoft Office
D- Browser security plug-ins that limit pop-up execution, browser scripting, Java, Java script, and other add-ons that can compromise browser security.
E- Intrusion detection - With the gap in antivirus, companies need to better prepare for compromise and increase their detection capabilities of signs of compromise and attacks. Detection is the single most effective way to address compromise and active attacks.

Unfortunately, the key is to know WHAT TO LOOK FOR (i.e. Indicators of Compromise). This is why there has been a rise in prominence and need for detection expertise and post-breach response companies like Grayhat, Mandiant, Proviti, and Kroll.

Companies have not been successful detecting attacks and compromise, and are being told by external sources (mostly law enforcement) that they were compromised. The following reports all state this trend:

Reference (Mandiant): https://www.mandiant.com/resources/m-trends/
Reference (Mandiant):
https://www.mandiant.com/news/release/mandiant-releases-annual-threat-report-on-advanced-targeted-attacks1/
Reference (Verizon Data Breach Investigations Report):
http://www.verizonenterprise.com/products/security/dbir/
Reference (Trustwave Global Security Report):
https://www2.trustwave.com/2013GSR.html

Some of the Mandiant report?s highlights include:
- Nearly 2/3 (63%) of organizations learn they are breached from an external source.
- 4 Years 10 Months - Longest time period Mandiant observed APT1 in a single victim's network
- 243 - median number of days that the attackers were present on a victim network before detection
- Targeted attacks continue to evade preventive defenses, but organizations are getting better at discovering them on their own.
Still, a full 63% of victims were made aware they had been breached by an external organization such as law enforcement.
- The typical advanced attack goes unnoticed for nearly 8 months.
- Attackers spend an estimated 243 days on a victim?s network before they are discovered ? 173 days fewer than in 2011. Though organizations have reduced the average time between compromise and detection by 40%, many are still compromised for several years before detecting a breach.
- Attackers are using comprehensive network reconnaissance to help them navigate victims? networks faster and more effectively.
- Attackers are frequently stealing data related to network infrastructure, processing methodologies, and system administration guides to gather the reconnaissance data they need to more quickly exploit network and system misconfigurations.

- Advanced Persistent Threat (APT) attackers continue to target industries that are strategic to their growth and will return until their mission is complete.
- Once a Target, Always a Target
- Organizations are being targeted by more than one attack group, sometimes in succession. In 2012, 38% of targets were attacked again once the original incident was remediated. Of the total cases Mandiant investigated in 2012, attackers lodged more than one thousand attempts to regain entry to former victims.

2012 Verizon Data Breach Investigations Report:
- 85% of breaches took weeks or more to discover
- 92% of incidents were discovered by a third party
- 84% - Availability of log evidence for forensics by percent of breaches (84% of companies compromised had the log evidence)

Trustwave Global Security Report Summary:
- In those cases in which an external entity was necessary for detection, analysis found that attackers had an average of 173.5 days within the victim's environment before detection occurred. Conversely, organization that relied on self-detection were able to identify attackers within their systems an average of 43 days after initial compromise.
- Businesses are slow to ?self-detect? breach activity. The average time from initial breach to detection was 210 days, more than 35 days longer than in 2011. Most victim organizations (64%) took over 90 days to detect the intrusion, while 5% took three or more years to identify the criminal activity.
- 33% detection was from law enforcement, 40% regulatory detection, and only 16% self detection

GRAYHAT assessment:
- Detection is broken for most companies.
- Companies are most likely told by outside entities, primarily law enforcement, that they were compromised.
- Companies cannot detect signs of compromise or attack, despite having the logs.
- Companies spend millions of dollars on intrusion detection equipment and they still cannot detect that they were hacked.
- Someone, perhaps the government, can help US critical infrastructure companies with indicators of compromise to look for signs of compromise.
- Critical infrastructure needs training and qualified people to detect compromise or signs of attack.
- The government needs to enable better detection practices and/or incentize companies to increase this capability.
- Someone, perhaps government, should test a company's effectiveness in detecting attacks (compulsory vulnerability scanning and penetration testing regime).

The consistent trend in each of the security reports over the past half decade are that adversaries are exploiting vulnerabilities in the following software products to compromise client platforms:
Oracle Java
Adobe Flash
Adobe Reader

Adobe PDF
Microsoft Office

Attacks are against:
1. Browsers of all types (i.e. Internet Explorer, Firefox, Mozilla, 2. Microsoft Office products that have enabled macros to launch the most compromised products listed above.
3. Operating system flaws are still a point of attack.

Example of this assessment, 0-day attack at Adobe Reader within days of Mandiant APT1 report:
http://www.seculert.com/blog/2013/02/spear-phishing-with-mandiant-apt-report.html

Trustwave Global Security Report Summary:
- Basic security measures are still not in place. ?Password1? is still the most common password used by global businesses. Of three million user passwords analyzed, 50% of users are using the bare minimum.
- Of all client-side attacks observed, 61% targeted Adobe Reader users via malicious PDFs.
- Always the two most noteworthy methods of intrusion, SQL injection and remote access made up 73% of the infiltration methods used by criminals in 2012.

2012 Verizon Data Breach Investigations Report:
- 79% of victims were targets of opportunity
- 96% attacks were not highly difficult
- 97% of breaches were avoidable through simple or intermediate controls
- Please see Table 8, Top 10 Threat Action Types by number of breaches and records for Larger Organizations and Smaller Organizations.
- Much more thorough industry analysis and metrics collected than DoD for Consensus Audit Guidelines / SAN 20

GRAYHAT Assessment:
1. Default and simple passwords still need to be addressed.
2. We need to enable strong passwords and password aging.
3. We need to test for weak passwords through vulnerability management programs.
4. Remote Access continues to be a huge point of compromise in most enterprise networks.
5. We need to use unbiased data to assess top RISKS and Threats than indicated by SANS 20 (iPost data is inconclusive, it uses McAfee EPO data which is flawed since it relies on broken antivirus detection data).

2. What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?

GRAYHAT RESPONSE

Trustwave Global Security Report Summary:
- Retail businesses and their sensitive data are back in the crosshairs. For the first time in three years, the retail industry made up the highest percentage of investigations at 45%.
- Web applications have now emerged as the most popular attack vector.
E-commerce sites were the No. 1 targeted asset, accounting for 48% of all investigations.
- Businesses are embracing an outsourced IT operations model. In 63% of incident response investigations, a major component of IT support was outsourced to a third party. Outsourcing can help businesses gain effective, cost-friendly IT services; however, businesses need to understand the risk their vendors may introduce and proactively work to decrease that risk.
- Businesses are slow to ?self-detect? breach activity. The average time from initial breach to detection was 210 days, more than 35 days longer than in 2011. Most victim organizations (64%) took over 90 days to detect the intrusion, while 5% took three or more years to identify the criminal activity.

- By reviewing the various industry reports, different sectors are being attacked differently.
- Different flaws are being exposed.
- 15 years ago, firewall, antivirus, and patching were all that were needed for "basic hygiene." The world has changed.
- Default accounts and simple passwords are an issue
Example:
http://www.eweek.com/networking/zombie-attack-warnings-broadcast-after-emergency-alert-system-hack/
- Hardened configurations are needed (see Center for Internet Security
standards)
- Firewalls and network segregation/isolation are still good practice
- Patching at the operating system and application level are still paramount, but so is pressure on vendors to do what Microsoft did in
2002 with Trustworthy Computing

3. Describe your organization's policies and procedures governing risk generally and cybersecurity risk specifically. How does senior management communicate and oversee these policies and procedures?

GRAYHAT RESPONSE

FAIR
ISO 31000
ISO 27005
Octave Allegro

We need to apply more than consequence.
We have industry data on probability (likelihood).

See:
http://datalossdb.org
http://www.privacyrights.org

See all of the security reports (i.e. Mandiant, Trustwave, Verizon, Symantec, Websense, etc.)
- Know bias of various reports and metrics collected
- Metrics sway how people apply security controls

4. Where do organizations locate their cybersecurity risk management program/office?

5. How do organizations define and assess risk generally and cybersecurity risk specifically?

GRAYHAT RESPONSE

Very few companies assess cyber risk and impact to others in cyberspace.

Most companies are looking to make profit and security tends to lag, especially basic hygiene. Example, voting machine weaknesses have been know for a decade.

6. To what extent is cybersecurity risk incorporated into organizations' overarching enterprise risk management?

7. What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?

GRAYHAT RESPONSE

Many companies lack the knowledge, discipline, or executive-level support and resources to implement FISMA or ISO/IEC 27001:2005 certification.

2012 FISM Report top reported cyber security challenges were:
- Funding the administration's priority initiatives (funding)
- Cultural challenges (culture that want convenience more than security...see RSA hack 2011, Symantec hack, Bit9 hack of 2013, etc.)
- Upgrading legacy technology (legacy technology is difficult to replace, resources no longer knowledgeable to solve issues if a re-write is needed and there's no funding to fix legacy)
- The current budget structure (funding again)
- Acquiring skilled personnel (overstated issue, we're lazy and convenience is king)

8. What are the current regulatory and regulatory reporting requirements in the United States (e.g. local, state, national, and
other) for organizations relating to cybersecurity?

GRAYHAT RESPONSE

None.

Many financial services organizations are buried with FFIEC compliance and other financial assessments to truly address security.

Most manufacturing, Internet, and retail companies have no security reporting requirements.

SOX reporting is not helpful for security.

SEC reporting guidelines issued in 2012 have not been adopted.

9. What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?

GRAYHAT RESPONSE

Information Technology is at the core of cyber security and the Internet.
Information Technology is what connected networks together through Internet Service Providers (ISPs).
Information Technology and vendors of Information Technology are responsible for vulnerabilities to their products.
Customers of Information Technology must follow the security guidance of their Information Technology vendor.

We are all reliant on Information Technology.

We are all reliant on Information Technology vendors.

We are all responsible for our Information Technology.

10. What performance goals do organizations adopt to ensure their ability to provide essential services while managing cybersecurity risk?

GRAYHAT RESPONSE

Many companies use annual, quarterly, and monthly industry benchmarks to gauge their security programs.

They use consulting firms like KPMG, Accenture, E&Y, PWC, and Deloitte to benchmark their security against their industry segment.
CSO Magazine and PWC conduct an annual Global State of Information Security that helps benchmark security programs:
http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml
There are other benchmarking programs available such as the Corporate Executive Board's IREC:
https://www.irec.executiveboard.com/Public/Default.aspx

11. If your organization is required to report to more than one regulatory body, what information does your organization report and what has been your organization's reporting experience?

12. What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cybersecurity conformity assessment?
Use of Frameworks, Standards, Guidelines, and Best Practices

GRAYHAT RESPONSE

International Organization for Standardization (ISO) is the defacto global leader.

As set forth in the Executive Order, the Framework will consist of standards, guidelines, and/or best practices that promote the protection of information and information systems supporting organizational missions and business functions.

NIST seeks comments on the applicability of existing publications to address cybersecurity needs, including, but not limited to the documents developed by: international standards organizations; U.S. Government Agencies and organizations; State regulators or Public Utility Commissions; Industry and industry associations; other Governments, and non-profits and other non-government organizations.

NIST is seeking information on the current usage of these existing approaches throughout industry, the robustness and applicability of these frameworks and standards, and what would encourage their increased usage. Please provide information related to the following:

1. What additional approaches already exist?

2. Which of these approaches apply across sectors?

3. Which organizations use these approaches?

4. What, if any, are the limitations of using such approaches?

5. What, if any, modifications could make these approaches more useful?

6. How do these approaches take into account sector-specific needs?

7. When using an existing framework, should there be a related sector-specific standards development process or voluntary program?

8. What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?

9. What other outreach efforts would be helpful?
Specific Industry Practices

In addition to the approaches above, NIST is interested in identifying core practices that are broadly applicable across sectors and throughout industry.

NIST is interested in information on the adoption of the following practices as they pertain to critical infrastructure components:

Separation of business from operational systems;

GRAYHAT RESPONSE

This is one of the single most important controls to implement, but very difficult to implement in most organizations.
This control is the basis for PCI DSS, but is offset using tokenization.

Use of encryption and key management;
Identification and authorization of users accessing systems;
Asset identification and management;
Monitoring and incident detection tools and capabilities;

GRAYHAT RESPONSE

- Monitoring and incident detection tools and capabilities is one of the biggest areas that GRAYHAT recommends.
- Advanced attacks like water holing are mitigated with a good detection strategy for this compromise.
Reference:
http://threatpost.com/en_us/blogs/large-scale-water-holing-attack-campaigns-hitting-key-targets-092512
- It also acts as a defense in depth strategy if companies fail to prevent or implement necessary security controls.
- Detection also reduces an attacker's dwell time once they compromise a network.

Incident handling policies and procedures;
Mission/system resiliency practices;
Security engineering practices;
Privacy and civil liberties protection.

1. Are these practices widely used throughout critical infrastructure and industry?

GRAYHAT RESPONSE

- We have detected much variance on how the Internet is protected.
- Heterogeneous security approaches as saved the Internet from collapse.
- We recommend diversity in security measures through people, process, and technology.

2. How do these practices relate to existing international standards and practices?
- International standards such as ISO provide a level of guidance to secure networks, while leaving some room for interpretation on the exact control.
- ISO also provides a means to measure maturity through ISO/IEC 21827:2008, which specifies the Systems Security Engineering - Capability Maturity Model (SSE-CMM).

3. Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure?

GRAYHAT RESPONSE

- All critical infrastructure relies on routing and DNS. Much of the Internet is connected via BGP and DNS, so we recommend hardening these
2 core services for everyone.
- Access to the admin control plane is also very important. If an attacker does not have access to manage a critical infrastructure system, then they will have a hard time compromising that system.
- We recommend that we do not directly expose critical infrastructure to the Internet. Ensure that it's firewalled. Ensure that admin privileges are secured.

4. Are some of these practices not applicable for business or mission needs within particular sectors?

GRAYHAT RESPONSE

- We need to think holistically. Controls that protect the cyber ecosystem are of utmost importance.

- DNS and routing are at the core of how networks interconnect.

- Passwords and identity are the foundations of security for cross sector access.

5. Which of these practices pose the most significant implementation challenge?

GRAYHAT RESPONSE

- Administrative and privileged access
- Network segmentation

6. How are standards or guidelines utilized by organizations in the implementation of these practices?

7. Do organizations have a methodology in place for the proper allocation of business resources to invest in, create, and maintain IT standards?

GRAYHAT RESPONSE

- No, most don't care. Security is an after thought and simply viewed as non-critical.
- We need to reinforce that companies have a responsibility to establish due care and a minimum safety standard for Internet security.

8. Do organizations have a formal escalation process to address cybersecurity risks that suddenly increase in severity?

9. What risks to privacy and civil liberties do commenters perceive in the application of these practices?

10. What are the international implications of this Framework on your global business or in policymaking in other countries?

GRAYHAT RESPONSE

- Several countries have adopted ISO 27001 certification as the minimum standard for security. These countries tend to score highest in overall security practices.
- By adopting an international security standard such as ISO, we are automatically aligned with other countries and their security protocols.
- We would like to be better informed about how other "international"
standards like SANS 20 obtained their claims for security. The number of countries and groups within other countries that adopted their standard appears suspect. Their exposure reduction claims are also suspect. Let's see the proof in their controls efficacy.

11. How should any risks to privacy and civil liberties be managed?

GRAYHAT RESPONSE

- Through public discourse.

12. In addition to the practices noted above, are there other core practices that should be considered for inclusion in the Framework?

GRAYHAT RESPONSE

- Today the cyber security framework and information sharing conversations seems to be discrete. Information sharing needs to be integrated into the cyber security framework
- At best, information sharing should be automated with the cyber security framework. For example, DHS Joint Intelligence Bulletins
(JIB) should be automated to work with other event correlation and SIEM or GRC type technology to simplify receiving information and acting on it.
- There is a lot of confusion on information sharing and reporting in the EO, who to report to, who is doing what, and roles and responsibilities. DHS should consider developing a RACI chart.

- Many companies are also not compelled to share vulnerability or compromise information. Many often threaten legal action to squash vulnerability and compromise reporting from reaching the public or even private vulnerability information sharing sites. This has to change.
- The debate on full disclosure must come to the forefront for information sharing to succeed.
- Incentives are required for companies to self report.

- We also need a common reporting, event recording, and incident reporting framework.
- Verizon developed Vocabulary for Event Recording and Incident Sharing (VERIS) that we should all standardize on:
http://securityblog.verizonbusiness.com/tag/incident-response/
- Standardizing incident recording, event information, and incident tracking allows all of us to benchmark ourselves against those like Verizon that publicly report breaches and post investigation findings.
It also allows us to add to their metrics and reporting structure, We can compare if we measure incidents and events in a similar manner.

- We need to continue to use of Mitre's vulnerability Common Vulnerability Scoring System (CVSS), Common Vulnerabilities and Exposures (CVE), and Common Weakness Enumeration (CWE) and the NIST National Vulnerability Database. It has been a staple for the Internet at large for a long time.

- We need to leverage US-CERT to alert companies and individuals on what needs to be done. For example, we should be alerting people now about the Open Relay issues associated with DNS and recommend, if not mandate, that users or the vendor automatically update BIND to the latest version to minimize the impact of the recent DDOS attacks.

GRAYHAT LLC