



Top Critical Controls In E-services Security

Saleh M. Al-Ghamdi

Information Technology

Saudi Aramco

March 22-24, 2010

Agenda

- Objective
- Security Highlights
- Threats Trend
- Potential Cyber Threat Sources
- Why these controls are important
- Top Security Controls
 - Objective of these control
 - Compromise lack of control
 - Implementation
- Recommendations
- Conclusion

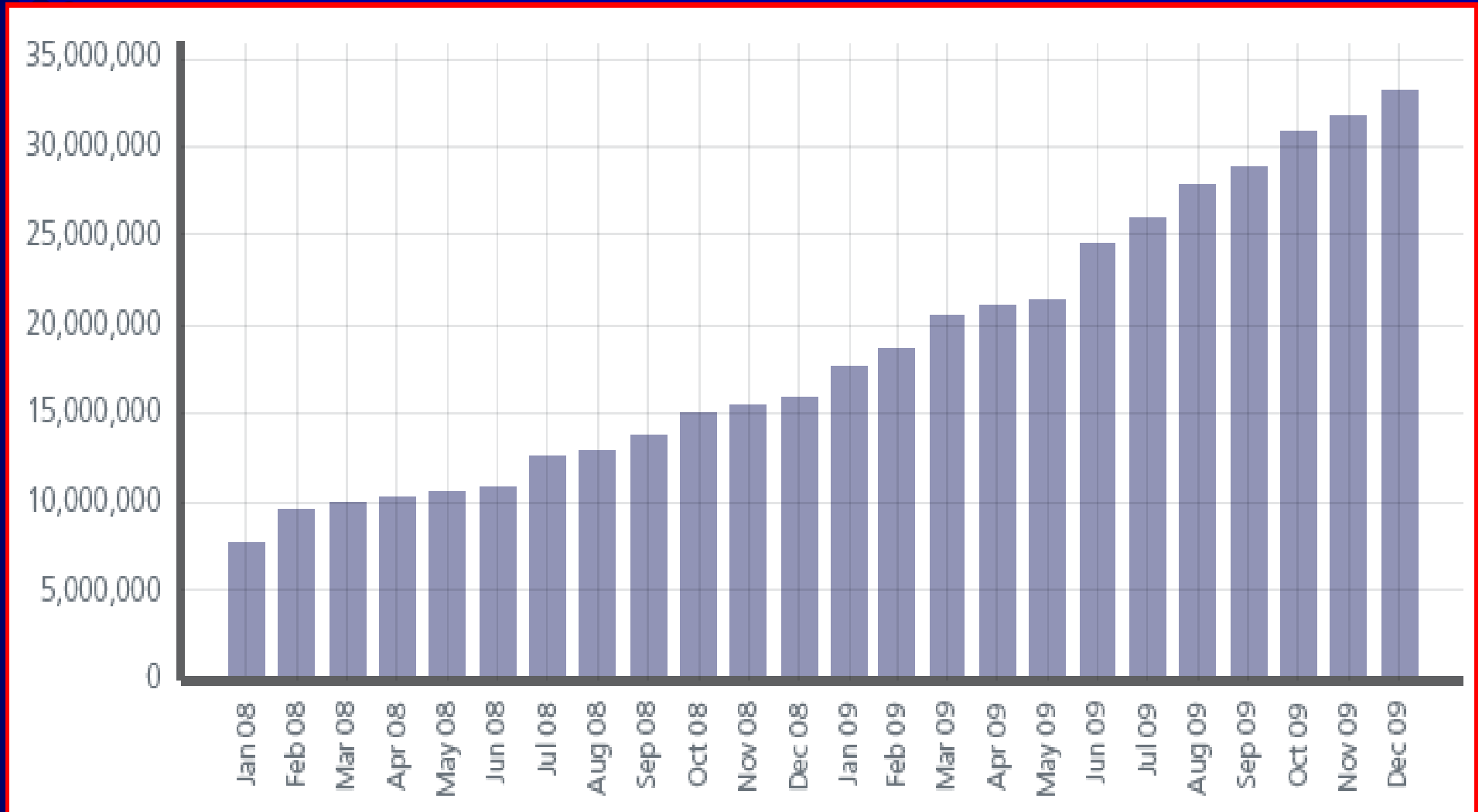
Objective

To share with you some critical security controls in the e-Services environment that organizations need to prioritize and follow to protect against threats and to meet security requirements defined by policies, standards, or regulations.

Security Highlights

- Operation Aurora:
 - It was a coordinated attack which included a piece of code that exploits the Microsoft Internet Explorer vulnerability to gain access to computer systems.
 - It was originated in China and aimed to hit Google and dozen of other organizations (e.g. Yahoo, Symantec,).
 - Operation Aurora is changing the cyber threat landscape once again.
 - These attacks have demonstrated that companies of all sectors are very lucrative targets.
- Zero day attack:
 - Zero-day attack is a computer threat to exploit vulnerabilities that don't have fix yet.
 - hackers are becoming faster at exploiting a vulnerability
- Securing organizations against cyber attack become one of the highest priority
- There is a need to establish security control to ensure information are effectively protected against vulnerabilities, attacks and exploitation.
- Regulations require organizations to protect against cyber attacks

Threats Trend - Malware



Potential Cyber Threats sources

- Internal
 - Legitimate clients
 - Government users or their representatives
 - Insiders
- External
 - Hostile outsiders
 - Criminal organizations
 - Foreign intelligence services
 - Commercial organizations
 - Investigation agencies
 - Terrorist organizations

Why These Controls are Important

- Cyber security is getting more complicated every day.
- Companies are being compromised.
- CIO need prioritized controls to get most ROI.
- Agreement is needed between:
 - Auditors
 - System Administrators (operations)
 - Security staff
- Organizations need to stop people from violating systems and compromising the confidentiality, integrity and availability of their data.
- We need a metric and measurement that everyone can agree to use.
- These critical security controls were agreed upon by knowledgeable individuals and teams from:
 - Department of Defense
 - U.S. Department of Energy
 - Others
 - U.S.-CERT
 - Civilian penetration testers
 - FBI



Top SANS

Critical Security Controls

Top SANS Critical Security Controls

- Hardware and Software Inventory
- Secure Configurations for
 - Hardware and Software
 - Network Devices such as Firewalls, Routers and Switches
- Boundary Protection
- Audit Logs Maintenance, Monitoring and Analysis
- Applications Security
- Administrative Privileges Control
- Vulnerability Assessment
- Malware Defenses
- Control of Network Ports, Protocols and Services
- Wireless Control

Objective of These Critical Controls

- Have automated reports generated when :
 - new devices are connected to the network
 - new software is installed
 - configurations are changed.
- Trend reporting for management.
- Proper configuration control and traffic monitoring
- proper tracking of critical data
- Detect attackers if they can not be prevented (Prevention is ideal but detection is a must)
- identify unauthorized access
- Minimize compromise
- Timely identification and remediation of high risk vulnerabilities
- prevent malware (viruses and spyware)

Hardware and Software Inventory

How lack of this control is compromised:

Hardware:

- Scan and identify new connected system.
- You can not protect system you don't know.

Software:

- Attackers can find vulnerabilities in the S/W.
- Unauthorized S/W can easily contain:
 - Known vulnerabilities:
 - Un-patched system.
 - Mis-configured system.
 - Zero day vulnerabilities:
 - Extraneous software, services and sample script.

Hardware and Software Inventory

Implementation:

Hardware:

- Deploy automated asset inventory discovery tool.
- Maintain asset inventory of all connected system.
- Ensure inventory monitoring tools are operational.
- Organizations must establish assets owner.

Software:

- Device list of authorized software for each system.
- Deploy software inventory tools.
- Develop software white-listing technology.

Secure Configurations for Hardware and Software

Compromise:

- Default installation tend to have services turned on.
- Default installation have installed components that are not required.
- Two main cause of compromise:
 - Un-patched system.
 - Most default images loaded is not updated on a regular basis.
 - Mis-configured devices.
 - Attackers break in though open ports and vulnerabilities.
 - Extraneous service create additional entry points.

Secure Configurations for Hardware and Software

Implementation:

- System images must have documented security setting.
- Standardized images should represent hardened version of the underlying OS.
- Change management system should be used to approve and document any deviation from standards.
- Government agencies should negotiate contract to buy systems configured securely out of the box using standard images.
- Provide regular charts for executives.
- Implement, deploy and test a vulnerability monitoring system.

Secure Configurations on Network Devices

Compromise

- Network devices often have unsecure configurations:
 - Default configurations are normally un-patched and have known vulnerabilities.
 - Default admin accounts and password are used.
- Network devices often unprotected and sit in front of firewall.
- Compromised network devices can be used to sniff, modify or redirect traffic.

Secure Configurations on Network Devices

Implementation:

- Create secure configuration. Any deviation should be approved, documented, and recertified regularly.
- Use two-factor authentication and encryption for managing network devices.
- Create separate network connections for management of the network infrastructure.
 - Utilize VLANs to create isolation.
- Apply principle of least privilege to all network devices.

Boundary Protection

Compromise:

- Attacker focus on exploiting internet facing systems:
 - Automated tools like Core Impact and Meta-Sploit can be used to exploit vulnerable entry points into network.
- Extranet can be used to tunnel into non-secure network.
- Attackers can sneak in malware via e-mail.

Boundary Protection

Implementation:

- Deploy IDS/IPS on the boundaries and between critical networks:
 - At least packet header information should be recorded.
- Filter outbound traffic:
 - All outgoing traffic goes through proxy. Proxy support includes:
 - Logging individual access.
 - Block specific URL, domain name, and IP addresses.
 - Block access to malicious Web site.
 - White list support.
- Use two-factor authentication for all remote access.
- Develop plan to rapidly deploying filters for virus outbreak.

Audit Logs Maintenance, Monitoring and Analysis

Compromise:

- Deficiency in security logging allow attackers to hide their location and malicious software.
- Attackers rely on the following facts:
 - Most organizations don't maintain or archive log files, so there are now way to find out what attacker did.
 - Log files are not centrally logged so they can be deleted or modified.
- Rootkits are automated way to cover attacker track.

Audit Logs Maintenance, Monitoring and Analysis

Implementation:

- OS should be configured to log events associated with access attempt.
- All access to critical information must be logged.
- Control access to logs.
- Use Security Event and Information Management (SEIM) to help correlation and analysis automation.
- All critical servers should have detailed logging.
- All logs should be centrally maintained in a central server.

Applications Security

Compromise:

- Attackers can exploit vulnerabilities exist in application and custom code.
- In-house developed codes are not maintained and tested by software vendors.
- More than 70 new vulnerabilities per week make an easy point of access.
- Organizations don't have patch management process for all software (e.g., QuickTime, Media Players, ... etc.).
- Attackers can inject specific exploit, including buffer overflow, SQL injection, and cross-site scripting code to gain control over vulnerable machines.

Applications Security

Implementation

- Organizations should test in-house and third party developed application for any vulnerability.
 - Work with developer for in-house code.
 - Work with vendor for third party application.
- Use Web application scanner.
- Deploy Web application firewalls.
 - Inspect all web application traffic.
 - Identify common attacks (XSS, SQL injection, Buffer overflow).
- Software should run with minimal privilege.
- Any extraneous code should be removed.

Administrative Privileges Control

Compromise:

- Misuse of admin privileges.
- Opening malicious mail attachments.
- Downloading and opening file from a malicious Web site or simply visiting malicious Web site.
- Elevation of privilege.
- Local admin privilege:
 - User installed a software that is actually spyware or Trojan.
 - User installed software that allow attackers remote access.
 - Users change firewall setting.

Administrative Privileges Control

Implementation:

- Inventory of all admin accounts.
- Change default password before deploying new devices.
- All password should be encrypted/hashed.
- Limit the use of admin accounts.
- Use two-factor authentication for all admin account.
- Segregate admin access based on roles:
 - Workstations admin, Domain admin, Database admin.
- Audit admin access:
 - Monitor for anomalous activity.
 - Track suspicious behavior.
 - Reconfiguration of devices, account creation, access list change.

Vulnerability Assessment

Compromise:

- Any public reported vulnerability can be exploited by attacker.
- Patch list is the vendor admitting to vulnerability.
- The longer a system is not patched the greater the chance an attacker will exploit it.
- Organizations that do not scan for vulnerabilities will have their system compromised.

Vulnerability Assessment

Implementation:

- Perform regular vulnerability scanning for all devices, systems and applications.
- Run vulnerability scanning in authenticated mode to overcome limitations of unauthenticated scanners.
- Deploy automated patch management tools.
- Share vulnerability report with senior management.
- Critical patches must be evaluated in test environment before deployment to production.
- Use specialized scanner for specific applications – Oracle.

Malware Defenses

Compromise:

- Users disable antimalware to install programs.
- Signature update are not performed regularly.

Malware Defenses

Implementation:

- Monitor workstations, servers, and mobile devices for active and up-to-date anti-malware.
- Disable all auto-run features - USB
- Configure automatic scanning.
- Deploy honeypot as detection mechanism to slow down attacker.
- Deploy NAC to verify security configuration before granting access to network.

Control of Network Ports, Protocols and Services

Compromise:

- Attackers scan systems and discover:
 - Open port
 - Running services
- Many software automatically install services and enable them by default - Administrators are not aware of these enabled services.

Control of Network Ports, Protocols and Services

Implementation:

- Deploy and configure network perimeter that allows only required and known type of network.
- Create and deploy rule set base on known traffic between all firewalls network.
- Employ default deny rule on host-based FW or port filtering tools on end systems.
- Use scanning techniques to identify open port and services.
- Implement hardening recommendations from guidelines such as NIST configuration guidelines.
- Operate critical services on separate physical host machines such as DNS, mail, database, ...

Wireless Control

Compromise:

- Use of Wired Equivalent Privacy (WEP) encryption instead of newer more secure protocols.
- Use of WiFi Protected Access (WPA) with weak encryption key.
- Use of open wireless network without personal security controls.
- Improperly configured wireless network card.
- No security implementation by user.
- Lack of physical security for the wireless device.

Wireless Control

Implementation:

- All wireless devices connected to the network should match authorized configuration and security profile.
- Use Wireless Intrusion Detection System (WIDS) to identify rogue wireless devices.
- Monitor all wireless traffic.
- Ensure all wireless traffic leverages at least AES encryption used with at least WPA2 protection.
- Ensure wireless network use authentication protocol such as EAP/TLS or PEAP – this provide credential protection and mutual authentication.
- Regularly, scan for unauthorized and mis-configured wireless infrastructure.
- Disable peer-to-peer wireless network capability on wireless client.
- Identify, develop and implement strong wireless policy.

Recommendations

- These controls can not be implemented in a year. You need to spend more time to implement. Evaluate these controls.
- These controls should be automated where feasible.
- These controls should be continuously and automatically measured
- Organization must ensure consistent controls across an enterprise to effectively detect/prevent attacks
- Negotiate Desktop standardization:
 - Security patch management and security configuration
 - Antimalware programs
 - Authorized and unauthorized applications

Conclusions

- Government and private sector are being attacked.
- These controls are not meant to supersede NIST guidelines.
- Organizations agreement on industry standards are essential.
- These controls are designed to help organizations that have different levels of information security capabilities.
- To help organizations focus on achieving baseline of security
- The real threat may not be the most obvious one.
- Attacks from authorized users are far more common than attacks by hackers.
- The automation of these Controls will radically lower the cost of security while improving its effectiveness.

References:

- SANS : Implementing Twenty Critical Security Controls for effective cyber defense and audit guidelines
- NIST: National Institute of Standards and Technology
- McAfee Threat Report

Thank you

ارامكو السعودية
Saudi Aramco

