States of Jersey Police

Making Jersey Safer

CYBER DEFENCE CRITICAL SECURITY CONTROLS

Please note that only the summaries of the top 20 critical security controls for cyber defence are available in this document.

Each of the 20 control areas includes multiple individual sub-controls that specify actions an organisation can take to help improve its defences. More information is available from the Centre for the Protection of National Infrastructure "Restricted" website at https://protect.cpni.gov.uk/Cyber-Security/critical-controls/in-depth/critical-control1/critical-control-1-advice-documents/. Please contact the CTSA at the States of Jersey Police for more information.

The 20 control areas and individual sub-controls focus on various technical aspects of information security, with the primary goal of helping organisations prioritise their efforts to defend against today's most common and damaging computer and network attacks.

Outside of the technical realm, a comprehensive security program should also take into account many other areas of security, including overall policy, organisational structure, personnel issues (e.g., background checks, etc.), and physical security.

To help maintain focus, the 20 controls do not deal with these important but non-technical aspects of information security. Organisations should build a comprehensive approach to these other aspects of security as well, but they are outside of the scope here.

In summary, the guiding principles used in devising the 20 control areas and their associated sub-controls include the following:

- Defences should focus on addressing the most common and damaging attack activities occurring today, and on those anticipated in the near future.
- Enterprise environments must ensure that consistent controls are in place across the organisation to effectively negate attacks.
- Defences should be automated where possible and periodically or continuously measured using automated measurement techniques where feasible.
- A variety of specific technical activities should be undertaken to produce a more consistent defence against attacks that occur on a frequent basis against numerous organisations.
- Root cause problems must be fixed in order to ensure the prevention or timely detection of attacks.

- Metrics should be established that facilitate common ground for measuring the effectiveness of security measures, providing a common language for executives, information technology specialists, auditors, and security officials to communicate about risk within the organisation.

The 20 controls presented here are also designed to support organisations with different levels of information security capabilities. To help organisations design a sound security baseline and then improve beyond that baseline, sub-controls included in each of the summaries of the 20 controls have been grouped into specific categories:

Quick wins

These fundamental aspects of information security can help an organisation rapidly improve its security stance generally without major procedural, architectural, or technical changes to its environment. It should be noted, however, that these sub-controls do not necessarily provide comprehensive protection against the most critical attacks. The intent of identifying “quick wins” is to highlight where security can be improved rapidly.

Improved visibility and attribution

These sub-controls focus on improving the process, architecture, and technical capabilities of organisations so that they can monitor their networks and computer systems and better visualise their own IT operations. Attribution is associated with determining which computer systems, and potentially which users, are generating specific events. Such improved visibility and attribution helps organisations detect attack attempts, locate the points of entry for successful attacks, identify already-compromised machines, interrupt infiltrated attackers’ activities, and gain information about the sources of an attack. In other words, these controls improve an organisation’s situational awareness of its environment. These sub-controls are identified in this document as “visibility/attribution.”

Hardened configuration and improved information security hygiene

These sub-controls are designed to improve an organisation’s information security stance by reducing the number and magnitude of potential security vulnerabilities and by improving the operations of networked computer systems. They focus on protecting against poor security practices by system administrators and end users that could give an adversary an advantage in attacking target systems. Control guidelines in this category are formulated with the understanding that a well-managed network is typically a much harder target for computer attackers to exploit. These sub-controls are identified in this document as “configuration/hygiene.”

Advanced

These sub-controls are designed to further improve the security of an organisation beyond the other three categories. Organisations already following all of the other sub-controls should focus on this category.

In general, organisations should compare all 20 control areas against their current status and develop an organisation-specific plan to implement the controls as a critical component of an overall security program. Ultimately, organisations should

strive to implement each control area, applying all of the sub-controls within each area, and working from quick wins through visibility/attribution, configuration/hygiene, and up to advanced. As a start, organisations with limited information security programs may want to address the quick wins sub-controls in order to make rapid progress and build momentum within their information security program.

Many of these controls can be implemented and measured using existing tools found in many government agencies and corporations. Other controls can be implemented using commercial or, in some cases, free, open-source software. Still others may require an investment in new enterprise tools and personnel expertise.

Each control area also includes a metric section that provides detailed information about the specific timing and objectives associated with the most important elements of the given control. Each control area also includes a test section that provides information about how organisations can evaluate their implementation of each control metric. These tests are devised to support automation wherever possible so that organisations can achieve reliable, scalable, and continuous measurements of their adherence to the controls and related metrics.

Critical control 1: Inventory of authorised and unauthorised devices

Summary

Reduce the ability of attackers to find and exploit unauthorised and unprotected systems. Use active monitoring and configuration management to maintain an up-to-date inventory of devices connected to the enterprise network, including servers, workstations, laptops, mobile, and remote devices.

Critical control 2: Inventory of authorised and unauthorised software

Summary

Identify vulnerable or malicious software to mitigate or root out attacks. Devise a list of authorised software for each type of system, and deploy tools to track software installed (including type, version, and patches) and monitor for unauthorised or unnecessary software.

Critical control 3: Secure configurations for hardware and software on laptops, workstations, and servers

Summary

Prevent attackers from exploiting services and settings that allow easy access through networks and browsers. Build a secure image that is used for all new systems deployed to the enterprise, host these standard images on secure storage servers, regularly validate and update these configurations, and track system images in a configuration management system.

Critical control 4: Continuous vulnerability assessment and remediation

Summary

Proactively identify and repair software vulnerabilities reported by security researchers or vendors. Regularly run automated vulnerability scanning tools against all systems and quickly remediate any vulnerability - with critical problems fixed within 48 hours.

Critical control 5: Malware defences

Summary

Block malicious code from tampering with system settings or contents, capturing sensitive data, or spreading. Use automated anti-virus and anti-spyware software to continuously monitor and protect workstations, servers, and mobile devices. Automatically update such anti-malware tools on all machines on a daily basis. Prevent systems from using auto-run programs to access removable media.

Critical control 6: Application software security

Summary

Scan for, discover, and remediate vulnerabilities in web-based and other application software. Carefully test internally developed and third-party application software for security flaws, including coding errors and malware. Deploy web application firewalls that inspect all traffic, and explicitly check for errors in all user input (including by size and data type).

Critical control 7: Wireless device control

Summary

Protect the security perimeter against unauthorised wireless access. Allow wireless devices to connect to the network only if they match an authorised configuration and security profile and have a documented owner and defined business need. Ensure that all wireless access points are manageable using enterprise management tools. Configure scanning tools to detect wireless access points.

Critical control 8: Data recovery capability

Summary

Minimise the damage from an attack: Implement a trustworthy plan for removing all traces of an attack. Automatically back up all information required to fully restore each system, including the operating system, application software, and data. Back up all systems at least weekly; back up sensitive systems more often. Regularly test the restoration process.

Critical control 9: Security skills assessment and appropriate training to fill gaps

Summary

Find knowledge gaps, and fill them with exercises and training. Develop a Security Skills Assessment program, map training against the skills required for each job, and use the results to allocate resources effectively to improve security practices.

Critical control 10: Secure configurations for network devices such as firewalls, routers, and switches

Summary

Preclude electronic holes from forming at connection points with the Internet, other organisations, and internal network segments: Compare firewall, router, and switch configurations against standards for each type of network device. Ensure that any deviations from the standard configurations are documented and approved and that any temporary deviations are undone when the business need abates.

Critical control 11: Limitation and control of network ports, protocols and services

Summary

Allow remote access only to legitimate users and services. Apply host-based firewalls and port-filtering and scanning tools to block traffic that is not explicitly allowed. Properly configure web servers, mail servers, file and print services, and domain name system (DNS) servers to limit remote access. Disable automatic installation of unnecessary software components. Move servers inside the firewall unless remote access is required for business purposes.

Critical control 12: Controlled use of administrative privileges

Summary

Protect and validate administrative accounts on desktops, laptops, and servers to prevent two common types of attack: (1) enticing users to open a malicious e-mail, attachment, or file, or to visit a malicious website; and (2) cracking an administrative password and thereby gaining access to a target machine. Use robust passwords that follow known standards.

Critical control 13: Boundary defence

Summary

Control the flow of traffic through network borders, and police content by looking for attacks and evidence of compromised machines. Establish multi-layered boundary defences by relying on firewalls, proxies, demilitarised zone (DMZ) perimeter networks, and other network-based tools. Filter inbound and outbound traffic, including through business partner networks (“extranets”).

Critical control 14: Maintenance, monitoring and analysis of audit logs

Summary

Use detailed logs to identify and uncover the details of an attack, including the location, malicious software deployed, and activity on victim machines. Generate standardised logs for each hardware device and the software installed on it, including date, time stamp, source addresses, destination addresses, and other information about each packet and/or transaction. Store logs on dedicated servers, and run biweekly reports to identify and document anomalies.

Critical control 15: Controlled access based on the need to know

Summary

Prevent attackers from gaining access to highly sensitive data. Carefully identify and separate critical data from information that is readily available to internal network users. Establish a multilevel data classification scheme based on the impact of any data exposure, and ensure that only authenticated users have access to non-public data and files.

Critical control 16: Account monitoring and control

Summary

Prevent attackers from impersonating legitimate users. Review all system accounts and disable any that are not associated with a business process and owner. Immediately revoke system access for terminated employees or contractors. Disable dormant accounts and encrypt and isolate any files associated with such accounts. Use robust passwords that follow known standards.

Critical control 17: Data loss prevention

Summary

Stop unauthorised transfer of sensitive data through network attacks and physical theft. Scrutinise the movement of data across network boundaries, both electronically and physically, to minimise the exposure to attackers. Monitor people, processes, and systems, using a centralised management framework.

Critical control 18: Incident response capability

Summary

Protect the organisation’s reputation, as well as its information. Develop an incident response plan with clearly delineated roles and responsibilities for quickly discovering an attack and then effectively containing the damage, eradicating the attacker’s presence, and restoring the integrity of the network and systems.

Critical control 19: Secure network engineering

Summary

Keep poor network design from enabling attackers. Use a robust, secure network engineering process to prevent security controls from being circumvented. Deploy network architecture with at least three tiers: DMZ, middleware, private network. Allow rapid deployment of new access controls to quickly deflect attacks.

Critical control 20: Penetration tests and red team exercises

Summary

Use simulated attacks to improve organisational readiness. Conduct regular internal and external penetration tests that mimic an attack to identify vulnerabilities and gauge the potential damage. Use periodic red team exercises — all out attempts to gain access to critical data and systems — to test existing defences and response capabilities.

PO BOX 789 JERSEY JE4 8ZD TELEPHONE 01534 612612
FAX 01534 612612
WEBSITE www.Jersey.Police.uk EMAIL sojp@jersey.pnn.police.uk