CYBER ESSENTIALS

COMPLIANCE STANDARD

osirium.com

OSIRIUM

HOW OSIRIUM HELPS ADDRESS

CYBER ESSENTIALS COMPLIANCE

INTRODUCTION

The Cyber Essentials scheme has been developed by Government and industry to identify a set of standard requirements for mitigating the risk from the most common Internet-based threats.

By implementing the required controls, and complying with the Cyber Essentials assurance framework, organisations should be able to mitigate against the majority of the most successful cyber attacks targeting UK businesses.

Cyber Essentials concentrates on five key controls that address boundary checks, the secure configuration of systems, access control, malware protection and the need for patch management.

Compliance with the Cyber Essentials controls will help organisations mitigate common threats such as the risk of malware propagated through phishing, and hacking through the exploitation of known vulnerabilities in servers and devices.

Malware and hacking are both so dangerous because they typically exploit weaknesses in passwords hygiene.

Passwords are required to access critical infrastructure as well as desktop and laptop devices. If a threat activist successfully extracts a password through a piece of malware or by leveraging standard passwords on a server, they will subsequently be able to extract data of value from the organisation.

Malware infections almost always take place at the desktop. However, most sensitive data or critical systems are separated and protected by privileged accounts and passwords. It's these credentials that hackers are looking for at your end points. By making those passwords as complex as possible, changing them as often as possible and separating them from your users wherever possible, you're able to break the entire kill chain very quickly.

Osirium's PxM Platform helps organisations manage the use of passwords for access to critical infrastructure. This is known as Privileged Access Management (PAM). Implementing a PAM solution can help an organisation to address several controls within Cyber Essentials.

Control 1: Boundary Firewalls and Internet Gateways

Section 1.1 states that the default administrative password for any firewall or equivalent network device should be changed to an alternative, strong password.

The PAM module of Osirium's PxM Platform solution takes firewall access to a higher security level. The PxM Platform can be used to change the default administrator password and manage the password lifecycle. The PxM Platform can be used to securely store and encrypt the administrator password. The PxM Platform can also use the maximum password complexity supported by the firewall, and automatically refresh the password in accordance with the organisation's password management policy. In operation, the PxM Platform injects the privileged password on behalf of the administrator when access to the firewall is required. This means that the administrator password is never shared with the user and thus cannot be shared, stolen, or extracted by malware.

Cyber Essentials proposes that firewall administration interfaces should not be addressable from the internet. However, where management of the firewall is outsourced to a third party organisation, it should be protected by additional security arrangements.

Osirium's PxM Platform is commonly used to control access to critical infrastructure from third-party organisations. The PxM Platform can control access by obfuscating the administrative password, tying access to a valid change ticket, limiting access to a time window, and by presenting the third party administrator with access only to the tasks they are authorised to carry out on the target server.
The PxM Platform can also be used to record the third party session which is important from an audit perspective.

Control 2: Secure Configuration

Computers and network devices should be configured to reduce the level of inherent vulnerabilities. Most computer and network devices come with a standard configuration which includes an administrative account and user accounts, all of which will have standard passwords.

These default configurations provide cyber attackers with an opportunity to gain unauthorised access.

Cyber Essentials requires unnecessary administrative accounts to be removed or disabled. Furthermore, any default password for a user account should be changed to an alternative strong password.

Osirium's PxM Platform automatically scans and detects user accounts on all critical infrastructure devices under management. Accounts are flagged for attention, giving administrators the option to delete, lock, approve or manage those accounts going forward.

Approved and managed accounts are monitored and audited to track the last use date, allowing notifications to be triggered after a defined period of inactivity so they can be removed or disabled. Moving accounts into a managed status also ensures that the passwords are changed and refreshed to maximum supported complexity.

Control 3: User access control

Cyber Essentials dedicates one of the five controls to user access control and pays particular attention to the risk posed by privileged accounts. Privileged accounts are used to gain access to critical infrastructure such as Windows servers, routers, firewalls and database servers.

Because they are used to access the most sensitive resources, privileged accounts create a security headache and need to be protected to the highest possible degree.

Privileged account credentials are at risk from the same threats that target standard user passwords. Phishing attacks may be deployed to attempt to extract password credentials by deceit and malware is commonly used to identify instances of password entry and then share this information with a threat activist who may then leverage the credentials to exfiltrate data of value from the organisation.

The insider threat is also a serious concern for organisations. The press is ripe with stories of disgruntled employees who turn against their employer and use their privileged status to attack critical infrastructure.

But the insider threat is not limited to people with malintent. Many insider breaches originate from good intentions or poor process.

It is common practice for administrators to tokenise passwords. This is a process used to standardise passwords and make them easy to remember. An example would be to select a memorable word such as favourite football team and then add the current year. Every month, when the password must be changed, the month can be appended. For example, Liverpool_2017_3 would be changed to Liverpool_2017_4 and so on.

The problem with passwords that are easy to remember is that they are easy to hack.

Then there is the matter of how to control the use of privileged passwords. Many organisations will store privileged passwords in plain text format. When a password is required, it can be obtained from the password store and used.

The password file may be encrypted while at rest, but when the password is required it must be typed into the endpoint device, making it prone to malware, RAM scraping, shoulder surfing and other threats.

And then there is the matter of password sharing and shared account access. When administrators share passwords, it prevents an organisation from being able to audit actions and associate hem to specific individuals.

Further, the more people who know a password, the greater the risk of it being exposed.

To address all of these real risks, Cyber Essentials documents seven steps to protect against the misuse of privileged credentials.

a. All user account creation should be subject to a provisioning and approval process.

b. Special access privileges should be restricted to a limited number of authorised individuals.

c. Details about special access privileges (e.g. the individual and purpose) should be documented, kept in a secure location and reviewed on a regular basis (e.g. quarterly).

d. Administrative accounts should only be used to perform legitimate administrative activities, and should not be granted access to email or the internet.

e. Admin accounts should be configured to require a password change on a regular basis (at least every 60-days).

f. Each user should authenticate using a unique username and strong password before being granted access to applications, computers and network devices.

g. User accounts and special access privileges should be removed or disabled when no longer required (e.g. when an individual changes role or leaves the organisation) or after a pre-defined period of inactivity (e.g. 3 months).

These steps are all extremely important to mitigate the risks posed by misuse of privileged account credentials, but the real challenge in meeting these seven steps is in how to do it in an effective manner.

Lets take an organisation with ten administrators and 250 servers and a 60-day password change policy as an example. To comply with the Cyber Essentials Guidelines, ten staff with access to 250 servers would require 2,500 privileged accounts. The privileged passwords would need to be changed six times in a year so that requires 15,000 distinct passwords to be used during a twelve-month term.

This level of complexity presents an operational nightmare for organisations and helps to demonstrate why administrators attempt to tokenise and simplify their passwords.

Osirium provides a technology solution to this challenge with the PAM Module of its PxM Platform.

Osirium enables organisations to control all instances of privileged access to critical infrastructure. Acting as a proxy between administrators and the servers they administer, Osirium's PxM Platform is primarily used to store privileged credentials and manage the full lifecycle of the passwords.

As a result, the PxM Platform removes the need for passwords to be known, changed and controlled by the administrators themselves.

Osirium's PxM Platform can be used to provision and subsequently deprovision individual administrator accounts on every system under management. Furthermore, access policies can be built to only grant access for specific users to specific accounts rather than using generic administrator level accounts that grant access to the whole estate.

Osirium's PxM Platform also provides a Privileged Task Automation engine that allows organisations to control administrative access to allow only very specific and limited abilities to execute pre-defined admin tasks without granting full direct access to systems in question. Task Automation upholds the principle of 'least privileged access' to a level beyond normal access control methods and tools.

Because the PxM Platform operates as a proxy for all privileged access, all administrative connections are tracked and audited with the ability to report against exactly who has what access at any given point in time.

Administrative accounts should not be used to gain access to the internet and so to prevent this a dual account model must be implemented. Osirium's PxM Platform builds on this principle by providing the ability to automatically translate from standard to privileged accounts for a user access session without them needing to know the privileged account password.

Osirium's PxM Platform can be configured to grant each privileged user their own unique admin accounts with the associated passwords being refreshed as often as desired. Dormant accounts can be flagged for attention and subsequent removal. In parallel, because the PxM Platform can authenticate users against Active Directory, a disabled AD account would automatically prevent access to a privileged account by association.

Building larger firewalls does not address the complexity of modern cyber threats. Privileged access management solutions help organisations to protect the resources that matter most to them. When access is controlled with Osirium's PxM Platform, localised instances of malware, and even the most sophisticated phishing attempts become blunted. This is because the passwords required to access the most valuable resources no longer need to be remembered, shared or entered into an endpoint device.

About Osirium

Osirium is a UK software development team that has pioneered the concept of a virtual air gap for privileged account access. The team have delivered a virtual appliance that can recognise an incoming identity, create a connection to a system, device or application, perform single sign-on and enterprise class password life cycle management, and then hand the pre-prepared session back to the incoming request ready for system management.

The session can be recorded, subject to time windows and device group separation. Osirium has delivered millions of privileged tasks and sessions for many of our blue chip clients. Osirium currently has four patents pending.

11-13 High Street, Theale
Reading RG7 5AH

0118 324 2444
osirium.com