Acronis



WHITE PAPER

Essential Eight Cybersecurity Mitigation Strategies White Paper by Acronis



Table of contents

Introduction 3

Objective of this white paper 3

What are the Essential Eight Mitigation Strategies? 4

About 4

Why the Essential Eight Mitigation Strategies are important 4

Essential Eight Maturity Levels explained 13

Beyond the Essential Eight with Acronis 14

Acronis and Information Security Manual (ISM) 14

References 14

Copyright © 2002-2023 Acronis International GmbH.

Introduction

Acronis Cyber Protect Cloud is at the forefront of the latest technologies and innovative solutions that will protect your organisation now and in the future. Whether businesses and MSPs are establishing fundamental security or further developing maturity, advanced threats remain constant.

Recent examples of cyberthreats include large-scale attacks, like REvil ransomware, targeting managed service providers (MSPs) and impacting thousands of their customers. (Justice, n.d.) Research indicates the number of cyberattacks per organisation has increased 24% this year (Acronis Mid-Year Cyberthreats Report).

The consequences of an attack could spell the end of an organisation due to financial, reputational and operational losses.

The risk of cybersecurity threats has not diminished and will continue to grow in the future, with more sophisticated attacks and more disruptions to businesses and MSPs across the world that have left their systems and devices open to vulnerabilities.

Objectives of this white paper

This white paper has been prepared to give the reader an understanding and demonstration on how Acronis aligns with the Essential Eight Mitigation Strategies (E8) coupled with our strengths against the different levels of the E8 Maturity Model and beyond.

The E8 framework empowers organisations with the know-how to improve cyber resilience, accelerate security maturity, and guarantee the baseline of preventative cybersecurity measures are met. These strategies serve as a resource for small to medium-sized businesses and MSPs, outlining standards to ensure businesses adopt a layered approach to security and draw awareness to the need for integrated security tools. When these tools work together, they reduce the number of network vulnerabilities adversaries use to thwart and circumvent legacy antivirus software.

In this white paper, learn how Acronis enables businesses and MSPs to follow the Essential Eight framework and reach a high maturity level with integrated cybersecurity, backup and management capabilities. We will take you on your journey towards developing your own Essential Eight Mitigation Strategies, plus share Acronis' unique strengths supporting the Information Security Manual (ISM) mitigation strategies, a framework that works with a company's risk management plan.

Information Security Manual (ISM) explained

The Australian Cyber Security Centre (ACSC) developed the Information Security Manual (ISM) as a comprehensive framework designed to assist Australian government agencies and businesses in protecting valuable information, systems and digital infrastructures from cyberattacks. One of the key components of the ISM is the E8 Mitigation Strategies, which outlines actionable and practical steps that organisations, like service providers and their clients, can implement to enhance their cybersecurity posture.



Copyright © 2002-2023 Acronis International GmbH.

What are the Essential Eight Mitigation Strategies?

About

The Essential Eight Mitigation Strategies (E8) is a cybersecurity framework developed by the ACSC to define technical recommendations for enhancing cyber maturity on Microsoft internally-connected environments.



Figure 1. The Essential Eight Mitigation Strategies

The E8 specifies strategies designed to protect an organisation from over 80% of cyberattack techniques.

Why the Essential Eight Mitigation Strategies are important

The E8 defines a layered approach to enhancing cyber maturity. The model is designed as a prescriptive tool to communicate the importance of taking multiple steps to reduce the spread of attacks. Each layer covers aspects of a business, including organisational processes, technologies, human factors and communication. Layering security measures, designed to work together, creates a more effective "barrier" against cyberthreats, individuals and organisations to ensure the security of critical data and safeguard business continuity. The model illustrates that no single layer of protection is foolproof, but by adding security layers in alignment with the Essential Eight Mitigation Strategies, an organisation can maximize cybersecurity effectiveness.

Copyright © 2002-2023 Acronis International GmbH.

Prevent

Strategy 1: Application control

The ACSC defines application control as, "the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets is prevented on workstations from within standard user profiles and temporary folders used by the operating system, web browsers and email clients." In other words, Strategy 1: application control involves satisfying criteria for creating blocklists (a list of unapproved applications) and allowlists (a list of approved applications) from executing on systems.

The importance of application control

Agreeing on a list of permitted applications (or a list of prohibited applications for that matter) is a common challenge most MSPs and businesses face. Once properly set up, application control critically reduces your risk of application-based threats introduced through the execution of unvalidated programs.

Acronis and the Essential Eight Strategy

Acronis restricts the execution of malicious executables. Moreover, Acronis solutions can blacklist certain apps and stop the execution of unauthorized applications. Acronis logs execution events on workstations and internet-facing servers which can be collected for compliance, cyber insurance and executive reporting. Acronis satisfies regulatory compliance that requires application controls such as PCI DSS, HIPAA and others.

Key takeaways

Implementation

Restrict access to unapproved applications or allow access to trusted applications

Threats prevented

Prevent the execution of malicious apps which introduce malware into your network

How Acronis helps

Log application execution events to help your organisation satisfy regulatory compliance, qualify for cyber insurance and strengthen security maturity

Application control includes three maturity levels defined in the table below:

Level 1	Level 2	Level 3
The execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets is prevented on workstations from within standard user profiles and temporary folders used by the operating system, web browsers and email clients.	*Includes all level one requirements and the below: Application control is implemented on workstations and internet-facing servers Allowed and blocked executions on workstations and internet-facing servers are logged	*Includes all level one and two requirements and the below: Microsoft's 'recommended driver block rules' are implemented Application control rulesets are validated on an annual or more frequent basis (period validation) Event logs are protected from unauthorised modification and deletion Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected

Copyright © 2002-2023 Acronis International GmbH.

Prevent

Strategy 2: Patch applications

Cybercriminals leverage security vulnerabilities to exploit and compromise networks. Regular vulnerability scans identify flaws within security systems and patches are applied to protect networks from exploitation. From productivity suites, web browsers and their extensions, email clients, PDF software and security products, patching applications reduces your risk of compromise.

The importance of patching applications

Performing scanning and patching activities within a strict time frame strengthens organisational assets by expediting the resolution of security vulnerabilities that pose significant cyber risk to MSPs and businesses. Staying up to date can be a costly and resource-intensive process for most. However, automated tools can help identify all installed applications, scan for vulnerabilities and apply patches more efficiently, allowing security IT technicians to refocus more critical objectives, like monitoring, investigation and incident response.

Acronis and the Essential Eight

Acronis finds and identifies applications and patch levels, making it easy for system administrators to remove or keep them. Acronis performs network and active directory discovery supported in Windows environments. Discovery is automated and scheduled or initiated by the admin. Acronis vulnerability assessment runs on a schedule daily by default and vulnerability assessment (VA) data is updated every 3 hours by default, but can be changed by the admin. The default setting for patches to be approved in Cyber Protect is 7 days and can be changed by an admin.

Multiple levels of vulnerability patching exist. These are defined below:

Key takeaways

Implementation

Keep applications up to date and patch any unidentified vulnerabilities exposing you to exploitation

Threats prevented

Prevent vulnerabilities from being exploited that introduce malware to your network

How Acronis helps

Performs regular asset discovery and vulnerability assessments to identify, prioritize and patch known and previously unknown exposed vulnerabilities to keep your organisation up to date

Level 1

An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.

A vulnerability scanner is used at least daily to identify missing patches or updates for security vulnerabilities in internet-facing services.

Patches, updates or vendor mitigations for security vulnerabilities in internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists.

Level 2

*Includes all level one requirements and the below:

A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in other apps.

Patches, updates or other vendor mitigations for vulnerabilities in office productivity suits, web browsers and extensions, email clients, PDF software and security products are applied within two weeks of release. For vulnerabilities in other apps are applied within one month of release.

Level 3

*Includes all level one and two requirements and the below:

Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release, or within 48 hours if an exploit exists.

Applications that are no longer supported by vendors are removed.

Copyright © 2002-2023 Acronis International GmbH.

Prevent

Strategy 3: Configure Microsoft Office macro settings

This E8 Strategy involves disabling Microsoft Office macro settings to control and prohibit users from misuse. The Microsoft Office macro settings should be blocked on incoming emails or other methods of entry and enforce anti-malware scanning. E8 specifications include event logging of macros allowed and blocked, compiling an inventory of trusted publishers, validating these lists annually, and more.

The importance of configuring Microsoft Office macro settings

Through configuring Microsoft macros, MSPs and businesses ensure only trusted users, locations, documents, add-in catalogs and other macro settings are granted. Configuring Microsoft macro settings gives organisations and service providers control over autorun tasks that can introduce unwanted executions while maintaining user productivity and flexibility.

Acronis and the Essential Eight

Acronis solutions are compliant with the E8 strategy, Configure Microsoft Office macro settings. Registry settings can be set via Powershell script and Microsoft Office macros are disabled for unauthorized users. Acronis also ensures files originating from the internet are blocked, that macro security settings cannot be changed by users, and that antivirus scanning of macros is enabled.

Multiple levels of macro setting maturity exist. These are defined below:

Key takeaways

Implementation

Ensuring access to Microsoft Office macro settings are disabled or restricted from users

Threats prevented

Prevent unauthorized users from accessing, tampering or changing Microsoft Office macros with malicious intent

How Acronis helps

Restricts users from changing macro settings, avoids user misuse and functionally complies where other tools have been used to satisfy this mitigation strategy

Level 1

Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.

Microsoft Office macros in files originating from the internet are blocked.

Microsoft Office macro antivirus scanning is enabled.

Microsoft Office macro security settings cannot be changed by users.

Level 2

*Includes all level one requirements and the below:

Microsoft Office macros are blocked from making Win32 API calls.

Allowed and blocked Microsoft Office macro execution events are logged.

Level 3

*Includes all level one and two requirements and the below:

Only Microsoft Office macros running from within a sandboxed environment, a Trusted Location or that are digitally signed by a trusted publisher are allowed to execute and only privileged users responsible for validating macros are free of malicious code can write to and modify content within trusted locations.

Macros digitally signed by an untrusted publisher cannot be enabled via the Message Bar or Backstage View. Microsoft Office's list of trusted publishers is validated on an annual or more frequent basis.

Allowed and blocked Microsoft Office macro execution events are centrally logged. Event logs are protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when signs of compromise are detected.

Copyright © 2002-2023 Acronis International GmbH.

Protect

Strategy 4: User application hardening

User application hardening is an E8 Strategy that blocks the user from changing web browser security settings. The strategy defines restrictions on users' interactions in a Windows environment, including protection from exploited vulnerabilities of unsupported software and blocking ads running malicious scripts.

The importance of application hardening

Threat actors often use browsers and other standard applications to gain access to sensitive data. User application hardening reduces Microsoft Windows attack surfaces through mitigating vulnerabilities in unsupported or older versions of applications. User hardening ensures appropriate measures are in place such as blocking web browsers from processing Java and web ads from the internet, and blocking code injections.

Acronis and the Essential Eight

Acronis Cyber Protect Cloud is compliant with industry standards involving application hardening. Especially where the PowerShell is configured to use Constrained Language mode, Acronis lets you constrain Language mode and it can be specified in Cyber Scripting.

Multiple levels of application hardening maturity exist. These are defined below:

Key takeaways

Implementation

Restrict or block user access to potentially dangerous online applications

Threats prevented

Mitigate malware, like "malvertising" and other application-based threats from penetrating your network

How Acronis helps

Protect users' interactions in Windows environments and stops adversaries trying to evade application whitelisting measures

Level 1

Web browsers do not process Java from the internet.

Web browsers do not process web advertisements from the internet.

Internet Explorer 11 does not process content from the internet.

Web browser security settings cannot be changed by users.

Level 2

*Includes all level one requirements and the below:

Microsoft Office is blocked from creating child processes, creating executable content and injecting code into other processes.

Microsoft Office is configured to prevent activation of OLE packages.

ACSC or vendor hardening guidance for Microsoft Office and PDF software is implemented.

Microsoft Office security settings cannot be changed by users and PDF software is blocked from creating child processes.

PDF software security settings cannot be changed by users.

Blocked PowerShell script execution events are logged.

Level 3

*Includes all level one and two requirements and the below:

.NET Framework 3.5 (includes .NET 2.0 and 3.0) is disabled or removed.

Windows PowerShell 2.0 is disabled or removed.

PowerShell is configured to use Constrained Language mode.

Blocked PowerShell script execution events are centrally logged.

Event logs are protected from unauthorised modification and deletion.

Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.

Copyright © 2002-2023 Acronis International GmbH.

Protect

Strategy 5: Restrict administrative privileges

Restricting administrative privileges aims to limit the number of administrative accounts within an organisation's IT infrastructure to only a set of essential administrators. By doing so, the E8 strategy prevents cybercriminals from gaining unauthorized access to restricted accounts used to escalate privileges, evade detection and spread infection.

The importance of restricting administrative privileges

MSPs and organisations can effectively harden Windows administrative access. This greatly minimizes the attack surface to secure their network and manage cyber risk. In the event a user's account is compromised, restricting administrative privileges prevents adversaries from accessing restricted assets which can reduce the impact of financial and operational damage.

Acronis and the Essential Eight

Acronis Cyber Protect Cloud offers role-based access privileges and can separate administrator accounts from user accounts. Administrator and user events are logged in Acronis Cyber Protect Cloud so service providers and businesses can better identify patterns of suspicious activity on networks, which can lead to indicators of compromise (IOCs).

Multiple levels of restricting admin privileges maturity exist. These are defined below:

Key takeaways

Implementation

Securing office macros to define the location where macros can be run and ensure settings can be trusted by approved users

Threats prevented

Prevents unauthorized changes to macro settings and stops the manipulation of macros from running malicious code

How Acronis helps

Acronis is compliant with restricting administrative privileges and prevents unapproved admins from accessing restricted assets

Level 1

Requests for privileged access to systems and applications are validated when first requested.

Privileged accounts (excluding privileged service accounts) are prevented from accessing the internet, email and web services.

Privileged users use separate privileged and unprivileged operating environments. Unprivileged accounts cannot logon to privileged operating environments.

Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.

Level 2

*Includes all level one requirements and below:

Privileged access to systems and applications is automatically disabled after 12 months unless revalidated. Privileged access to systems and applications is automatically disabled after 45 days of inactivity. Privileged operating environments are not virtualised within unprivileged operating environments.

Administrative activities are conducted through jump servers. Credentials for local administrator accounts and service accounts are long, unique, unpredictable and managed.

Privileged access events, account and group management events are logged.

Level 3

*Includes all level one and two requirements and the below:

Privileged access to systems and applications is limited to only what is required for users and services to undertake their duties.

Privileged accounts are prevented from accessing the internet, email and web services.

Just-in-time administration is used for administering systems and applications. Windows Defender Credential Guard and Windows Defender Remote Credential Guard are enabled.

Privileged access events, account and group management events are centrally logged.

Event logs are protected from unauthorised modification and deletion. Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.

Copyright © 2002-2023 Acronis International GmbH.

Protect

Strategy 6: Patch operating systems

Operating systems are essential to controlling hardware, software and service. These are attractive targets for cybercriminals. When known vulnerabilities in operating system are overlooked, your security infrastructure is exposed to malicious threats. The Essential Eight Strategy of patching operating systems defines vulnerability scanning and patching operations.

The importance of patching operating systems

Failure to patch operating systems leaves MSPs and businesses susceptible to intrusions. Establishing a robust patch management process protects systems by reducing the risk of cyber incidents and strengthening cybersecurity posture. Automating this process can help streamline vulnerability scanning and patching of operating systems to ensure the application of patches is carried out promptly and consistently.

Acronis and the Essential Eight

Acronis provides user-initiated, automated network and active directory discovery supported in Windows environments. Flexible scheduling helps you determine the frequency of vulnerability assessments scans, which run daily by default. Additionally, the collected vulnerability assessment data is updated every three hours to ensure you have the latest information. Acronis finds and identifies operating systems and patch levels, making it easy to remove or keep them.

Key takeaways

Implementation

Keep operating systems up to date and patch any unidentified vulnerabilities exposing you or your clients to exploitation

Threats prevented

Prevent the exploitation of unpatched vulnerabilities on operating systems

How Acronis helps

Acronis finds and identifies OSs and patch levels. Decisions on whether or not to remove them lies with the system administrator

Multiple levels of patch operation maturity exist. These are defined below:

Level 1

An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.

A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.

A vulnerability scanner is used at least daily to identify missing patches or updates for security vulnerabilities in operating systems of internet-facing services.

A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in operating systems of workstations, servers and network devices.

Patches, updates or vendor mitigations for security vulnerabilities in operating systems of internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists.

Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within one month of release.

Operating systems that are no longer supported by vendors are replaced.

Level 2

*Includes all level one requirements and the below:

A vulnerability scanner is used at least weekly to identify missing patches or updates for vulnerabilities in operating systems of workstations, servers and network devices.

Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, servers and network devices are applied within two weeks of release.

Level 3

*Includes all level one and two requirements and the below:

Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, servers and network devices are applied within two weeks of release, or within 48 hours if an exploit exists.

The latest release, or the previous release, of operating systems are used.

Copyright © 2002-2023 Acronis International GmbH.

Protect

Strategy 7: Multifactor authentication

Multifactor authentication (MFA) provides an additional layer of protection beyond traditional username and password authentication. MFA is a method that requires users to enter two or more forms of identification before gaining access to accounts or systems. This E8 strategy is designed to safeguard against risks like phishing, compromised internet access, and secure access to data and software.

The importance of multifactor authentication

For small businesses, MSPs and other organisations, employing MFA prevents the unauthorized access of threat actors. This E8 strategy offers a critical line of defense against credential stuffing, brute force, phishing and other attacks. Additionally, MFA can safeguard against potential lateral movement within a network.

Acronis and the Essential Eight

Acronis is compliant with the multifactor authentication policy. MFA can be enforced to access the Cyber Protect Cloud solution using supported external authenticator apps such as Microsoft and Google Authenticator. Acronis records successful and unsuccessful 2FA events in the audit log.

Multiple levels of authentication maturity exist. These are defined below:

Key takeaways

Implementation

An extra layer of protection for remote logins

Threats prevented

An extra layer of protection for remote logins

How Acronis helps

Functionally compliant where other tools have been used to provide the MFA mitigation strategy

Level 1

Multifactor authentication is used by an organisation's users when they authenticate to their organisation's internet-facing services.

MFA is used by an organisation's users when they authenticate to third-party internet-facing services that process, store or communicate their organisation's sensitive data.

MFA (where available) is used by an organisation's users when they authenticate to third-party, internet-facing services that process, store or communicate their organisation's nonsensitive data, and is enabled by default for an organisation's nonorganisational users (but they can choose to opt out) when they authenticate to the organisation's internet-facing services.

Level 2

*Includes all level one requirements and the below:

Multifactor authentication is used to authenticate privileged users of systems.

Multifactor authentication uses either something users have and something users know, or something users have that is unlocked by something users know or are.

Successful and unsuccessful multifactor authentication events are logged.

Level 3

*Includes all level one and two requirements and the below:

Multifactor authentication is used to authenticate users of important data repositories.

Multifactor authentication is phishing resistant and uses either something users have and something users know, or something users have that is unlocked by something users know or are.

Successful and unsuccessful multifactor authentication events are centrally logged.

Event logs are protected from unauthorised modification and deletion.

Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.

Copyright © 2002-2023 Acronis International GmbH.

Recover

Strategy 8: Regular backups

The E8 strategy defines "regular backups" enabling efficient recovery following a cyber incident. These activities include backing up important data and assets. The E8 also specifies admin privilege restrictions to limit access to backups, monitor and protect event logs from unauthorized deletion or modification, and other stipulations.

The importance of regular backups

If a business — MSP or a client of an MSP — gets hit with ransomware, backups ensure important critical data, software and configuration settings are not lost and recovery can be performed in a timely manner. Maintaining up-to-date and securely stored backups greatly minimizes downtime, allowing organisations and MSPs to rapidly recover following cyberevents. Performing regular backups is a proactive approach which safeguards against unforeseen disruptions to operations and defends business continuity.

Acronis and the Essential Eight

Acronis provides award-winning backup, data protection and recovery. With Acronis cloud or Acronis Cyber Infrastructure, immutable backups are performed to ensure critical data is secure and cannot be altered, deleted or changed — remaining free from malware and other cyberthreats. Immutable backups can be set to either Governance Mode or Compliance Mode. Acronis delivers file-level, disk-level, image and application backups of popular workloads including Mac, Windows, Linux, Microsoft 365, Google Workspace, Hyper-V, VMware and more.

Multiple levels of backup maturity exist. These are defined below:

Key takeaways

Implementation

Ensure a recoverable copy of your data stays clean and up to date

Threats prevented

Reduce disruption from data loss and mitigate corruption of data due to ransomware

How Acronis helps

Acronis proactively secures data with immutable backups, data protection, monitoring, reporting and more

Level 1

Backups of important data, software and configuration settings are:

- Performed and retained with a frequency and retention timeframe in accordance with business continuity requirements
- Synchronised to enable restoration to a common point in time
- Retained in a secure and resilient manner

Restoration of important data, software and configuration settings from backups to a common point in time is tested as part of disaster recovery exercises.

Unprivileged accounts cannot access backups belonging to other accounts and are prevented from modifying and deleting backups.

Level 2

*Includes all level one requirements and the below:

Privileged accounts (excluding backup administrator accounts) cannot access backups belonging to other accounts.

Privileged accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups.

Level 3

*Includes all level one and two requirements and the below:

Privileged accounts (excluding backup administrator accounts) cannot access backups belonging to other accounts, nor their own accounts.

Unprivileged accounts are prevented from modifying and deleting backups.

Privileged accounts (including backup administrator accounts) are prevented from modifying and deleting backups during their retention period.

Copyright © 2002-2023 Acronis International GmbH.

Essential Eight Maturity Levels explained

The Essential Eight Maturity Model also defines four different maturity phases (maturity zero through maturity three) that organisations should self-assess. It should be noted that at maturity zero level, there is no capability in this space.

Each maturity level roughly translates into readiness or sophistication preparedness against an attack or attacker. The ACSC recommends achieving the same maturity level across all eight mitigation strategies before moving on to higher maturity levels. For example, businesses with a Maturity Level One in Application Control should not begin to enhance security measures toward Maturity Level Two until they have successfully achieved Maturity Level One across all seven remaining essential mitigation strategies.

Maturity levels One through Three focus on mitigating various levels of attack sophistication. The E8 Maturity Levels Zero through Three are summarized below.

E8 Maturity Level	Description	How to use
Maturity Level Zero	Indicates open weaknesses are present in the organisations' cybersecurity posture and a high susceptibility to attacks.	Maturity Level Zero reflects organisations with critically poor cyber resilience. These organisations have open vulnerabilities, lack essential security measures and are prone to exploitation.
Maturity Level One	Addresses unsophisticated and nontargeted attacks that likely take advantage of known vulnerabilities and leverage public resources using common TTPs.	Maturity Level One is the foundational level of security in the ACSC Information Security Manual (ISM). It's the starting point for organisations to build their cybersecurity capability and improve their overall security posture.
Maturity Level Two	Addresses sophisticated and targeted attacks leveraging public resources and available tools to evade detection and security layers using tactics, like phishing and social engineering, to trick unsuspecting users.	At Maturity Level Two, MSP clients, like small and midsize businesses have established foundational security policies. At this level, organisations would have: • Developed a documented and communicated information security policy and conducted security awareness training for personnel, risk assessments and implementing risk treatment plans • Implemented access controls to limit access to sensitive information • Performed regular backups of critical data • Deployed anti-malware software and firewalls to protect ICT systems from external threats • Developed incident management and response procedures
Maturity Level Three	Addresses advanced persistent threats (APTs) and highly sophisticated attacks. These intrusions are targeted in nature, requiring advanced skills and techniques and are less reliant on public tools.	At Maturity Level Three, organisations have implemented a comprehensive and mature set of security controls that tailor to its specific risks and operational requirements. Organisations have established a culture of security awareness and continuous improvement, including the following: Regular security audits and assessments to identify vulnerabilities and areas for improvement Access controls and user management procedures to manage privileges and access to information and systems • Network segmentation and other network security controls to protect against advanced threats • Advanced security monitoring and incident response capabilities, including security information and event management (SIEM), security orchestration, automation and response (SOAR), endpoint detection and response (EDR), and extended detection and response (XDR) technologies • Regular penetration testing and vulnerability assessments (VAPT) to identify and address weaknesses • Well-structured incident response plan (IRP) and conducts regular exercises and testing

Copyright © 2002-2023 Acronis International GmbH.

Beyond the Essential Eight with Acronis

Acronis and ISM

Acronis Cyber Protect Cloud unifies backup, recovery, cybersecurity and endpoint management in one integrated solution. Acronis is the most reliable, efficient and easy way to protect business data with anti-malware and endpoint detection enhanced with machine intelligence, AI and behavioral-based technology against zero days, ransomware and sophisticated threats. Acronis helps service providers and businesses streamline cyber protection that leverages integration and automation to provide unmatched ease of use — reducing complexity while increasing productivity and decreasing operating costs.

Acronis is uniquely positioned to address more ISM mitigation strategies than any other vendor as shown in the table to the right:

Cycle	Complication
Prevent	Operating system patching
	Application patching
	Backup
	Immutable backups
	Secure scripting
	Hardware, OS and software application monitoring
	Vulnerability assessment
Protect	Email security
	URL filtering
	Antivirus, anti-malware, anti-ransomware
	Backup scanning for malware
	Data loss prevention (DLP)
Recover	Endpoint detection and response (EDR)
	Backup recovery / restore
	Disaster recovery



References

Acronis Cyber Protect Cloud . (n.d.). Prevent client downtime and data loss with essential cyber protection. Retrieved from Acronis Cyber Protect Cloud : https://www.acronis.com/en-sg/products/cloud/cyber-protect/

Australian Cyber Security Centre . (2017, June). Essential Eight Maturity Model. Retrieved from Australian Cyber Security Centre : https://www.cyber.gov.au/sites/default/files/2022-11/PROTECT%20-%20Essential%20Eight%20Maturity%20Model%20%28November%202022%29.pdf

Australian Cyber Security Centre . (n.d.). Strategies to Mitigate Cyber Security Incidents. Retrieved from Australian Cyber Security Centre : https://www.cyber.gov.au/acsc/view-all-content/strategies-to-mitigate-cyber-security-incidents

Australian Cyber Security Centre. (n.d.). Essential Eight Maturity Model. Retrieved from Australian Cyber Security Centre: https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model

Centre, A. C. (n.d.). Australian Cyber Security Centre Information Security Manual (ISM). Retrieved from www.cyber.gov.au: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism

CISA.gov. (n.d.). Protecting Against Cyber Threats to Managed Service Providers and Their Customers. Retrieved from cisa.gov: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-131a

Eric Swotinsky. (2022). Acronis Cyberthreats Report Year-end 2022: Data under attack. Retrieved from Acronis.com: https://www.acronis.com/en-us/blog/posts/acronis-cyberthreats-report-year-end-2022-data-under-attack/

Fleck, A. (2022, December 2). Cybercrime Expected To Skyrocket in Coming Years. Retrieved from Statista: https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/#:~:text=According%20to%20estimates%20from%20Statista's,to%20%2423.84%20trillion%20by%202027.

Furneaux, A. (n.d.). Building a Holistic Cybersecurity Program. Retrieved from Cyber Saint: https://www.cybersaint.io/blog/holistic-cybersecurity-program

Gartner. (2023). Learn From the WannaCry Ransomware Attack. Retrieved from Gartner: https://www.gartner.com/smarterwithgartner/learn-from-the-wannacry-ransomware-attack

https://www.awd.com.au/. (n.d.). Retrieved from awd.com.au.

Justice, D. o. (n.d.). Sodinokibi/REvil Ransomware Defendant Extradited to United States and Arraigned in Texas. Retrieved from The United States Department of Justice: https://www.justice.gov/opa/pr/sodinokibirevil-ransomware-defendant-extradited-united-states-and-arraigned-texas

Mackay, I. M. (2020, October 24). The Swiss cheese respiratory virus defense model for COVID19. Retrieved from figshare.com: https://figshare.com/articles/figure/The_Swiss_Cheese_Respiratory_Virus_Defence/13082618?file=25233461

National Institute of Standards and Technology . (2014, February 12). Framework for Improving Critical Infrastructure Cybersecurity. Retrieved from National Institute of Standards and Technology : https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf

National Institute of Standards and Technology . (n.d.). Cybersecurity Framework. Retrieved from National Institute of Standards and Technology : https://www.nist.gov/cyberframework

National Institute of Standards and Technology . (n.d.). Getting Started. Retrieved from National Institute of Standards and Technology : https://www.nist.gov/cyberframework/getting-started

NIST. (2021, January 25). Success Story: Saudi Aramco. Retrieved from NIST: https://www.nist.gov/cyberframework/success-stories/saudi-aramco

NIST. (n.d.). COMPUTER SECURITY RESOURCE CENTER - Defense in Depth. Retrieved from nist.gov: https://csrc.nist.gov/glossary/term/defense_in_depth

NIST Glossary. (n.d.). Retrieved from nist.gov: https://csrc.nist.gov/glossary/term/tactics_techniques_and_procedures

Reason, J. (2005). The Swiss cheese model of safety incidents: are there holes in the metaphor? Retrieved from ncbi.nlm.nih.gov: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1298298/

Security Magazine. (n.d.). Leading cyber risks & trends in 2022. Retrieved from Security Magazine: https://www.securitymagazine.com/articles/98695-leading-cyber-risks-and-trends-in-2022

Acronis

Learn more at
www.acronis.com

Copyright © 2002-2023 Acronis International GmbH. All rights reserved. Acronis and the Acronis logo are trademarks of Acronis International GmbH in the United States and/or other countries. All other trademarks or registered trademarks are the property of their respective owners. Technical changes and Differences from the illustrations are reserved; errors are excepted. 2023-09