THE ESSENTIAL EIGHT SECURITY CHALLENGE

Overcoming the roadblocks to implementing the ASD's recommended strategies.

The recent WannaCry and Petya ransomware outbreaks highlight the need for organisations to maintain good practice in the basics of cybersecurity. The fact that these global attacks could successfully exploit a known weakness – and one that was already patched – points to the immense security challenges organisations face.

The Australian Signals Directorate's (ASD) Essential Eight cybersecurity recommendations set out a series of strategies any organisation can follow to address these challenges.

But while the strategies appear both practical and obvious, applying those strategies isn't necessarily straightforward. Even seemingly simple recommendations on patch management, whitelisting and privileged account management can be stymied by a myriad of complications.

iTnews – in conjunction with information security provider The Missing Link – brought together IT and cybersecurity executives from leading Australian organisations to discuss how they were working to solve the various problems standing in the way of successful cybersecurity practices.

The roundtable discussion uncovered some insights into how Australian enterprises can address the challenges of implementing the ASD's Essential Eight strategies, along with IT leaders' ongoing concerns. And at top of the list of concerns is the growing and ever-evolving nature of security threats.

As Berys Amor, Director of Technology at Corrs Chambers Westgarth, said: "I think [the risk of data breach] is one of the biggest risks to any organisation. Cybersecurity is not set and forget – it's an ongoing program."

> "I think [the risk of data breach] is one of the biggest risks to any organisation. Cybersecurity is not set and forget – it's an ongoing program."
>
> *– Berys Amor, Director of Technology, Corrs Chambers Westgarth*

PATCH MANAGEMENT

Patch management is another major concern. The inability of so many organisations to patch their systems and avoid being infected by WannaCry or Petya highlights the seriousness of this problem.

The difficulty often stems from a simple lack of resources, coupled with the myriad of environments that organisations operate. The issue is not just one of running multiple operating systems and applications, but often different versions of those systems.

But the issue is not as simple as just applying the patches that are issued. And while the need to patch is clear, some technology professionals recall stories of applying a patch that interfered with systems performance – quickly drawing the ire of colleagues should business processes be affected. This leads to a need to balance the desire to patch quickly against that of maximising systems availability.

Moderator Brad Howarth and Berys Amor, Director of Technology, Corrs Chambers Westgarth

The problem of patch management can also be exacerbated by the age of the systems themselves. Many recent attacks have exploited older operating systems, which are often retained beyond their serviceable lifetime because the applications that run on them are of a similar vintage.

The dangers to system stability can be mitigated by using pre-testing solutions. Another option is to ensure sufficient redundancy, such that in the event of a problem with a patched system, the operating environment can immediately cut over to an unpatched redundant system until the patched system is stabilised. Such a strategy requires rigorous backup and testing procedures – which are also recommended in the ASD Essential Eight.

"I can't remember the last time we actually had a failure due to a patch," said Jason Blackman, CIO at Carsales.com. "Once you've got patching built into your deployment process, you've got a get-out-of-jail-free card. Rather than slow yourself down with all that testing for everything 'just in case', design a system that's resilient, that can take aggressive change and then test or slow down by exception as required."

ASSESSING PATCH CRITICALITY

The patching process can also be assisted through appropriate categorisation of the threat each patch remediates, such as through using the RACI (Responsible, Accountable, Consulted and Informed) matrix or the CVS (Common Vulnerability Scoring) developed by the PCI. This can allow an organisation to more accurately prioritise the true threat from a vulnerability and the subsequent urgency of remediation.

Jason Blackman, CIO, Carsales.com

For example, a vulnerability might be regarded as critical, but if that vulnerability has a known exploit, then it is classified as extra critical. If that vulnerability with a known exploit has malware in the wild, that's extra, extra critical.

Breaking criticality down into these three subsets allows priority to be given to the ones where malware is known to be exploiting it.

> "I can't remember the last time we actually had a failure due to a patch. Once you've got patching built into your deployment process, you've got a get-out-of-jail-free card."
>
> *– Jason Blackman, CIO, Carsales.com*

"That score is very much a raw score of the exploitability of that vulnerability. So what is the implementation of that within our organisation. Is it web facing? Is it not web facing? Is it a critical application or not? We do that asset correlation and then decide on the criticality," said Indy Delpachitra, Information Security Service Manager, Dulux Group.

The use of cloud-based services also provides another pathway for patch management. Most SaaS applications are, by default, the most up-to-date version of the software available, and require no external patch management. The use of cloud-based hosting can also give users the option of receiving the most up-to-date version of the client software through the cloud provider themselves, again reducing the need for patch management.

"That mitigates the patch management, because effectively, every day it's a new machine. We're constantly doing deployments, so when we do another deploy it'll bounce it up to the next available patched version. We rarely have a scenario where there has been a critical patch that we've got to do a deploy just for patch purposes'," said Blackman.

WHITELISTING

The process of certifying applications as safe may appear obvious, but the complexity and scale of some organisations can make even the apparently simple task of just identifying the applications used a difficult prospect. This process can be complicated further through the use of cloud-based tools and services, in the form of shadow IT.

While many organisations solve whitelisting by locking down employees into a standard operating environment, this can be difficult to both establish and maintain in some scenarios, such as when the organisation employs a large team of developers who have a tendency to use a wide range of tools.

Remedying such situations begins with effective monitoring of what is actually being used, then reducing this list to an approved set of applications.

"On the end-points, we have a fully locked down standard operating environment. In addition, we have a behaviour blocker in place which ensures that exploits are unable to be run on the end-point. We also have a behaviour monitor which monitors and alerts us if there is any anomalous, activity either on the network or on devices," said Ashutosh Kapse, Head of Cybersecurity & Technology Risk at IOOF Holdings.

Another recommended policy is to allow users choice, but to reduce the total choice down to applications that are both commonly-used and secure.

ACCOUNTING FOR THE HUMAN FACTOR

While technology plays a key role in enabling The Essential Eight, many of the problems it describes result from human behaviour.

"Cybersecurity is a leadership and a culture issue rather than a technology issue," said Kapse.

Workforce training and education is vital. One tool

Indy Delpachitra, Information Security Service Manager, Dulux Group

Ashutosh Kapse, Head of Cybersecurity & Technology Risk, IOOF Holdings

of particular benefit is the use of simulated phishing attacks, which can act as a guide to the success of cyber awareness training. Metrics to be tested might include the number of staff who opened the fake email, as even when email is not acted on, allowing images to download in the email can tell the attacker there is an actual person on the receiving end and hence confirm them as a target for future campaigns. Subsequently clicking the links in the email or opening attachments, or performing additional tasks such as entering credentials into a fake page, provides additional knowledge of how users might respond to actual attacks.

Opening, clicking and entering credentials all represent negative metrics, and the goal of training should be to drive these down to zero. But positive metrics are also important, such as the number of people who identify and report phishing campaigns and other suspicious activity. Reinforcement of this behaviour, through acknowledgement and rewards, can be used to drive this behaviour to 100 per cent.

"We have to encourage and reward reporting," said Phil Burg, Information Security Lead, Transformation & Technology at EnergyAustralia.

"Anytime someone reports a phish, whether it's a genuine one, or whether it's just something that looked like a phish, I email them back and tell them that we're only effective when people in the business are reporting. And I cc their boss on it. I get emails back from some of the managers saying, "Hey, that's really great. I'm going to recognise this person at our next team meeting'."

IOOF Holdings also rewards the right behaviour. "In order to see cultural change over time, organisations must encourage the right behaviours. We have an award called 'Successful Prevention of Cyber threat (SPOC)' award. We give this monthly to an employee who reports the most or something different or unusually suspicious," said Kapse.

Using this combination of testing and education has shown that negative metrics can be reduced by up to 70 per cent after a single attack, according to Aaron Bailey, CISO at The Missing Link.

GETTING HELP

The desire for many organisations to pursue digital transformation inevitably leads to greater potential exposure to cyber threats. Balancing the rewards against the risks requires a robust and effect approach to managing cyber threats, but to do so requires an investment in skills that many organisations struggle to afford, especially at a time when cyber skills are in high demand.

And regardless of the necessity of compliance and security, the natural tendency is to want to deploy skills to those projects that will assist with strategic goals such as customer experience and growth.

Given the clarity of the ASD Essential Eight, it is not surprising to see many organisations using it as their cybersecurity template. But despite its apparent simplicity, the underlying complexity of implementing its strategies means it is also not surprising to see them seeking external assistance to ensure they have all aspects covered.

Hence for mid-tier and large organisations alike, business priorities and resourcing constraints will lead many to consider outsourcing cybersecurity requirements, freeing staff up for tasks that will assist the organisation in its growth goals.

As one Australian IT executive said: "I don't want to outsource the entire IT department, but I do want to outsource the stuff nobody wants to do. No-one wants to do backup. No one wants to do patching. Antivirus is another boring one that's generally broken pretty much month to month. They're the classic things to put in managed services."

> "Cybersecurity is a leadership and a culture issue rather than a technology issue."
>
> *– Ashutosh Kapse, Head of Cybersecurity & Technology Risk, IOOF Holdings*

Security is often seen as an inhibitor, stifling productivity by limiting access to applications and administration rights or any number of activities that are demanded by the workforce. The challenge for security is to be a business enabler, accommodating the needs of users and allowing them to collaborate and use the devices they want, while not compromising security.

The ASD Essential Eight is a framework that can enable this. However, organisations need to have access to the resources and expertise to implement its strategies effectively – and if that can't be done internally, finding the right cybersecurity partner can help ensure the organisation has a secure and productive future.

About The Missing Link

The Missing Link is a premium provider of information technology solutions. Whether your requirements are enterprise-scale or a single office, you're seeking the same thing from your information technology provider – you'd like to be sure your systems are running reliably, cost-effectively, and delivering the business outcomes you've planned for.

The company provides information technology solutions across infrastructure, security, backup and disaster recovery, mobility, internet and communications, and cloud services.

The Missing Link is recognised as an industry leader and accredited to the highest levels in the design, delivery and support of the latest technologies.

The Missing Link's SmartSECURE® ASD8 as a Service delivers an architecturally designed fully managed service that adopts the Essential Eight ASD strategies, taking your current infrastructure and security posture to the next level.

The service has been developed to be cost effective when compared with in-house expenditure to implement the strategies; and pricing can be configured to meet your unique business needs. Whilst it is most effective to implement all eight strategies, the service is offered modularly, giving businesses the choice to only implement some or part of the strategies to complement existing technologies.

We have carefully selected leading enterprise-class vendors to ensure we can utilise the service across a heterogeneous environment including Microsoft, Apple, Unix and others.

About iTnews

This report was produced by the team at iTnews, Australia's most awarded technology publication for Australian business.

In an age when the right information at the right time can make or break a deal, Australia's technology leaders rely on iTnews for their daily fix of accurate, up-to-the-minute news, analysis and research.

Information and communications technology is the engine room of the modern business. Business leaders tell us they rely on iTnews to inform their strategy, make business cases for technology investments, set policies and chart their careers. Collectively, the team at iTnews has won a swag of awards which include Technology Title of the Year, Best News Title, Best Editor, Best Business Journalist, Best News Journalist and Best Technical Journalist.

The iTnews team also curates technology conferences and judges the annual Benchmark Awards for excellence in ICT project delivery.

themissinglink®

www.themissinglink.com.au

itnews FOR AUSTRALIAN BUSINESS

IBM®