As enterprises become more dependent on digital technologies, information security has become more vital in maintaining customer trust.
The days of set-and-forget security are gone. New online threats and new ways of doing business have put the onus on organisations to continually review, adapt and refine their tools and processes.

Our responsibility to protect business data and customer information becomes even more critical as digital technologies become more ingrained in our enterprises.

As with many other organisations, Optus’ digital capabilities are becoming ever more important to our customers and to our business. Almost by the day, we’re seeing more leads from our website, more downloads of our smartphone apps and more social media interaction with customers. Our business products are becoming increasingly tied to digital technologies, as we roll out more cloud services, more mobile applications and more web portals that provide vital reporting and account-management functions for our traditional telecommunications products.

Of course, being a major telco, security has always been a top priority for Optus, but now the stakes are even higher.

In this paper, we’ll offer some insights from the Optus Security Team into what it takes to build, maintain and evolve a carrier-grade information security practice – because that’s the level of protection that more and more enterprises will need to earn or maintain their customers’ trust.

New risks and threats

Businesses and government organisations alike are facing an ever increasing range of sophisticated threats, including distributed denial of service (DDoS) attacks, hacktivism, advanced persistent threats and targeted cyber-attacks.

Zero-day attacks – those that exploit previously unknown software vulnerabilities – are difficult to detect and are becoming more common. Advanced persistent threats (APTs) are another particularly sinister threat that typically target a single organisation. By using highly targeted intrusion techniques, APTs can bypass traditional signature-based security solutions. The attackers follow up with additional incursions over an extended period of time, until they achieve their objective – which is generally to infiltrate the organisation and quietly collect data.

APTs and other similar breaches can last for months. A recent study by Mandiant – the services division of security specialist company FireEye – showed that attackers were present on victim networks for a median of 229 days before being discovered. The longest presence was 2,287 days.¹

The attackers’ goals range from industrial espionage to damaging an organisation’s reputation. The media regularly reports on high-profile organisations that have been breached, exposing customer information such as credit card details. However, thousands of other attacks go unreported or even undetected every day.

According to another recent FireEye study, 97 per cent of organisations had been breached by at least one attacker bypassing all security layers. In three-quarters of the organisations, the perpetrator had control over the breached systems.²

With the new threats and greater business reliance on digital technologies, every enterprise needs to have the right security measures and strategies in place.

¹ Information Security Opinion Paper

² Information Security Opinion Paper
Our information security strategies

With the new threats and greater business reliance on digital technologies, every enterprise needs to have the right security measures and strategies in place.

At Optus, our information security strategy focuses on:
- early detection and incident response capabilities
- fostering a security-aware culture by educating our staff and customers
- leveraging relationships with our vendors, sharing information and collaborating on security related matters
- optimising our internal processes with regular audits, testing and reviews

Early detection of threats and vulnerabilities is critical. This requires advanced monitoring tools that constantly analyse data from detection points right across the network, so anomalies and potential threats are quickly identified. To this end, our security teams undergo regular training and keep up to date with the latest security intelligence.

With new threats like zero-day attacks and APTs, it’s also vital to continually educate and improve awareness among our staff and customers. It’s not easy for large organisations with lots of business units and management layers, therefore fostering a security-aware culture is critical.

Security testing and audits need to be performed regularly, whenever a new product is released and following any major change. Response plans need to be reviewed after every incident and continually fine-tuned. Eliminating false positives is also important to maximise security teams’ productivity and enable them to focus on genuine threats.

Protecting the weakest link

As the threats become more sophisticated, so too has security technology evolved, which is why attacks now typically target the weakest link in an enterprise – its people. Information security is now a social issue just as much as a technical one. Success relies on everyone doing their part, so it’s vital to get employee buy-in from the top down and right across the organisation.

Optus’ key security strategies include regular education programs. As a major telco, we’ve always had a security-conscious culture, so for us it’s a matter of maintaining vigilance by continually promoting good security practices and educating users about new threats. The discovery of new vulnerabilities such as Heartbleed – a bug in the encryption technology used by many e-commerce and transaction-based websites – drives home the importance of continually redefining people’s perception of what can be attacked and how.

Key recommendations

So after years of maintaining and evolving carrier-grade security systems and processes, what advice can Optus offer other enterprises seeking to develop similar levels of protection?

Most important is recognising that there is no simple solution. Information security requires a multi-layered, or otherwise known as a defense in-depth approach, that includes ongoing initiatives to educate users and cultivate a security-aware culture. Overlaying these efforts should be advanced technologies that provide strong layers of protection, and internal processes that safeguard against unauthorised network access and accidental disclosure of information. And given the rapidly evolving nature of online threats, it’s critical to continually review, adapt and refine security tools, processes and education campaigns.

The Australian Department of Defence (DoD) provides a list of essential strategies (see ‘The Department of Defence’s top security strategies’ on the right). Optus recommends implementing these strategies. The most critical are diligently patching operating systems and applications, and carefully managing users and access privileges.

Security as a competitive advantage

As if online threats aren’t enough, corporate compliance and governance responsibilities are increasing, with new rules such as Australia’s 2014 privacy law reforms.

However, our aim at Optus is go way beyond what the Privacy Commissioner and regulatory bodies require from us. That’s because we see information security not just as a responsibility, but also a competitive advantage, enabling us to build customer trust and confidence in us as an ICT provider.

We encourage our corporate and government customers to do the same, because information security provides the framework to better serve your customers and grow your business, by confidently bringing more digital services to market quickly.

The Department of Defence’s top security strategies

The Australian Department of Defence (DoD) has identified 35 strategies for mitigating targeted cyber intrusions, including four essentials:

1. Use application whitelisting of permitted or trusted programs to prevent execution of malicious or unapproved programs.
2. Patch applications such as Java, PDF viewers, Flash, web browsers and Microsoft Office. Patch systems with ‘extreme risk’ vulnerabilities within two days. Use the latest versions of applications.
3. Patch operating system vulnerabilities. Patch or mitigate systems with ‘extreme risk’ vulnerabilities within two days. Use the latest suitable operating system. Avoid Windows XP.
4. Restrict administrative privileges to operating systems and applications based on user duties. These users should use a separate unprivileged account for email and web browsing.

The DoD recommends that once the top four mitigation strategies have been implemented, organisations should select from an additional 31 strategies to address security gaps until an acceptable level of risk is reached. See www.asd.gov.au/infosec/top-mitigations/mitigations-2014-table.htm for the full listing.

Give us a call

To discuss how Optus can help you through advanced security solutions; contact your Optus Account Manager or call the Optus Business hotline on 1800 555 937

Join the conversation

@optusbusiness  yesopt.us/blog