IDC Analyze the Future

IDC ANALYST CONNECTION

Simon Piff
Associate Vice President, Enterprise Infrastructure
IDC Asia/Pacific

Vern-Harn Hue
Senior Market Analyst, Software (Security)
IDC Australia & New Zealand

Endpoint Security: A Primary Line of Defence in the Mobility Era

September 2013

The significance of both personal and mobile devices is apparent in today's business and technology environment. Fueled by the consumerisation of IT, we are entering the era of a three-device environment - laptops, smartphones and tablets. This, of course, will pose significant challenges and risks to the IT Manager as the "Bring-Your-Own-Device" (BYOD) trend also means that users are able to access corporate data and applications through their own mobile devices. Furthermore, the growth in both the volume and sophistication of attacks on networks and endpoints are also growing at an alarming rate. Organisations are looking for more comprehensive security solutions to address the new breed of security threats.

The following questions were posed by Optus Business to Simon Piff, Associate Vice President for Enterprise Infrastructure, IDC Asia/Pacific, and Vern-Harn Hue, Senior Market Analysis for Software Security, IDC Australia, on behalf of IT Directors and CIOs.

Q. Reading the press it would appear that IT security is not something that can be easily fixed as there is always a new virus, malware, method of hacking or data breach being reported almost daily. Is there any over-arching strategy that could be recommended with regards to this or is it simply futile?

A. Whilst IT security is not something one can easily fix in light of the changing nature of the internet, threats, and compliance needs; there are things which organisations can do in order to ensure that security across the IT infrastructure is managed.

The growing complexity of IT will require a new way of examining security. While security vulnerability is increasing at unprecedented rates in terms of the sophistication and severity of attacks, the reality is that most organisations are not keeping up with these malicious

actors. Moreover, today's corporate environment is further complicated by the bring-your-own-device (BYOD) phenomenon that is causing IT Manager's sleepless nights.

Relying on a single line of defence in today's IT environment is a flawed tactic, as a single line of security can potentially point to a single line of failure. Once the system is breached, the entire infrastructure is vulnerable. A 'defence in depth', or layered security approach is a method in which organisations use multi-layered technologies and policies to mitigate and prevent attacks. Typically, the layer of solutions would include automated patch-management solutions, End-user training, Firewall, Intrusion Prevention and Detection Systems, anti-virus and other protection applications. However, the pertinent conversation today should be to move away from point solutions towards a more connected and integrated security infrastructure which is architected to collect and share information. In any case, technology is only part of the equation. Proper policies and training should also be the hallmark of a strong security strategy. Security policies should be defined clearly to avoid ambiguity and in turn provide the organisation a clear and structured response in the event of a breach. Individuals should be provided with an adequate level of security awareness training. By providing them with the right guidance on protecting their personal and corporate data, it ensures that it will make it a step harder for the malicious actors.

Q. What does it take to strike a balance between engaging your employees by providing them with freedom and trust, and at the same time protecting your organisation?

A. Finding the balance between IT security and engaging or remaining relevant with your employees is a tricky balancing act. Whilst it is prudent to ensure your organisation and its data is secure, users who are entering the sales force today differ from their predecessors in their appetite for technology consumption and behaviour relating to data privacy. Organisation policies will have to adapt and address this, especially if they wish to engage with the younger workforce.

Younger users are typically less concerned about privacy due to their preferences towards accessing applications, and personal applications such as social media. They will typically test the boundaries of corporate policies as they believe in the freedom of device choice, mobile lifestyle and subsequently, the unrestrained use of social media sites.

From a training perspective, organisations must invest time and effort in providing information security training and education to their employees; to help them understand the risks and to provide benchmarks on how best to leverage the technologies that are provided to them.

From a technological aspect, organisations cannot rely on a single technology to address these problems. The most effective way of securing this environment is to identify roles, devices and applications; and to secure both the inbound and outbound access to the corporate network. The technology we have today also allows organisations to be more strategic in the way they look at applying granular controls over the user and applications. For example, organisations which allow the use of the internet for work purposes, could grant access to Facebook to monitor campaigns and customer sentiments; concurrently, administrators can deny access to games popular to social networking sites, such as "Angry Birds". Peer-to-peer applications may also be prohibited, but VoIP solutions such as Skype, might be authorised for business use. Policies could also be setup to provide access at lunchtime or during after-work hours and thus, allowing organisations to enforce security policies in ways that makes sense for their business.

Q. What are the best practices to ensure your organisation does not fall victim to social engineering attacks?

A. Social engineering is the art of manipulating people into volunteering information - such as, revealing confidential information and giving away computer access rights. Rather than using brute force to gain access, malicious actors leverage social engineering to trick users into disclosing sensitive and vital information. The most important aspect when dealing with social engineering attacks is to understand that there is not much difference between the techniques carried out by traditional fraud. By using a mix of user awareness, strong security policies and technologies, organisations can mitigate the risk of falling victim to social engineering.

Being constantly vigilant and maintaining a healthy level of scepticism is a good start. By restraining from the disclosure of confidential information unless it is verifiable, users can remain at least one step ahead of the malicious actors. Users should also undergo security training and be made aware of their duty towards protecting their customers' and organisation's data. As part of training, recognition of users who follow best practices can help reinforce behaviour. Designing internal security policies that are both brief and concise is also another important part of combating social engineering.

Having a centralised log of security events is one way to prevent a social engineering attack. Every time an employee requests to reset their password or is asked to divulge sensitive information, an event should be logged in this central log file, which feeds into a security incident and event monitoring (SIEM) tool. With the right information in the logs, patterns can quickly emerge, and in an attempt to access unauthorised information, IT security personnel can take action and even prevent the threats when they occur. The use of systems and approaches, such as multi-factor authentication and biometrics, can also deter and make it more difficult for malicious actors. For example, even if someone gains access to your username and password, a multi-factor authentication also requires you to hold two or more types of information to access the secured content.

Q. Security compliance has been at the heart of security strategies for the longest time. What new technologies or approaches can organisations deploy to further enhance, and reduce complexity when considering security compliance?

A. Information security and compliance is a complex melange of people, software, management and threats. Security compliance ensures that the practical needs of governance and enforcement of the security policy can be achieved. However, it also suffers from the misfortune of being a lot like haute couture, where the mode du jour (fashion of the day) dictates where the money gets invested and the constant change in the threat environment means that there is a lack of perceived continuity in long term investments, stymieing executive support. Using a compliance framework keeps technology, people and processes in check against a short term view of threat mitigation.

Compliance was developed with the idea of protecting the confidentiality and integrity of data in mind. While IT security grew as organisations were forced to meet auditory requirements, a "check-box" mentality also developed, with information security personnel becoming more concerned with ensuring their security controls met regulatory standards than with the security of their data. But this came at a cost, as these investments were not aimed at further improving the IT security infrastructure and understanding the upcoming threats on the horizon.

Being compliant itself; while doing the right thing, may not be enough to ensure that the organisation is secure from threats. The first step of any effective compliance exercise would be to first understand and identify the assets which are the most vulnerable and prone to attacks, as well as the current state of the security posture protecting these data and infrastructure. Organisations need to carry out regular risk-assessments to ensure that they understand the current vulnerabilities within their infrastructure. IDC believes that many organisations are now beginning to see the elephant in the room, and are responding in kind, by investing in the people, processes and technologies within their organisation. Using new technologies, such as security analytics, event correlation, and advanced malware detection and prevention will help to transition from a reactionary stance to a proactive defensive stance. Being a step ahead of the security curve does, after-all, tick the compliance box, but it also keeps you at the forefront of risk mitigation.

Q. I have been reading a lot about Advanced Persistent Threats, how different are these to the malware we face on a day-to-day basis and what can I do to ensure that my organisation is protected?

A. The term Advanced Persistent Threats (APT) was first used to describe state-sponsored cyber espionage, however, these attacks are also increasingly being geared towards organisations for financial gains. Unlike traditional malware that seeks to randomly infect endpoints using a specific exploit, APTs are sophisticated and advanced in nature and are also very stealthy, targeted and persistent; making it difficult for traditional security measures to identity and manage attacks. APTs also frequently rely on Zero-Day vulnerabilities in particular to launch highly targeted and tailored attacks on specific individuals. These attacks are difficult to detect, mitigate, and rectify and can sometimes lie dormant or stay on the target's network for long periods of time – even after the data is stolen and their mission is complete – to maintain surveillance and look for more valuable data.

With the proliferation of mobile devices, threats targeting the endpoint will continue to grow and place undue strain on signature-based malware as they try to keep up with the increasing numbers of threats. One must be cognisant that there is no single silver bullet solution to stop a determined malicious actor and that organisations will need to adopt a 'defence in depth' approach to reduce the risk of APTs.

Despite how daunting this may sound, doing the basics well can reduce the likelihood of these kinds of attacks. The first step is to better understand what your organisation is setting out to protect. Properly classifying and documenting confidential data in order to better compartmentalise vital assets is the first step in offering a resistance.

Once this is accomplished, organisations can then investigate solutions that provide behavioural heuristics, such as white-listing, and reputation services that can identify malicious content on the Internet and block access before it reaches the endpoint; as well as leveraging up to date methods such as scanning in the cloud. Other solutions such as Data-Loss Prevention (DLP) technologies and cloud-based sandboxing are also valuable additions in an organisations' arsenal. Organisations can also take further steps by utilising solutions that address role-based restrictions of administration rights, Network Access Controls (NAC), logging and monitoring capabilities that detect anomalous data-traffic and multi-factor authentication. To further ease the identity management across devices and applications, vendors have also introduced 'network administrative tools' that enable the enforcement of access and security policies for endpoint devices connected to an organisation's router and switch. This is another way of sustaining very granular controls over who has access to what

applications and data, and therefore, fulfilling many regulatory compliance requirements, simultaneously.

ABOUT THESE ANALYSTS

Simon Piff has more than 17 years of regional experience in the IT industry, serving in various sales and marketing management roles for hardware, software, services and online businesses. As Associate Vice President for IDC's Enterprise Infrastructure Research, Simon is responsible for the execution and delivery of the program focused on providing advice around the technologies that define enterprise infrastructure (servers, storage, networking and infrastructure software) and technology areas such as security, private cloud and virtualisation.

Vern-Harn Hue is a Senior Market Analyst for IDC Australia and New Zealand's (ANZ) software research. His research focus centres on Security Software, Appliances and Services. As part of his work, Vern conducts market analysis and forecasting for the Software and Appliance side of the research.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com