DATA MANAGEMENT

Travis Lee *indexes the latest trends in data security*

Most malware relies on unpatched software applications and unsupported operating systems

Thanks to rapid developments in storage and cloud technology, it has never been easier for organisations to collect, create and store data. The amount of data in the world has continued to grow exponentially for some time, and research from IDC predicts that approximately 50 zettabytes of data was created by the end of 2020, a figure that's set to triple by 2025.

Analysing datasets can deliver powerful business benefits, revealing insights that can help with key strategic decisions ranging from product launches to regional expansions. Combined with the relatively low cost of storage, this means businesses have long tended to habitually collect as much data as possible.

However, these expanding data footprints come with heightened risks. The 2020 Trustwave Global Security Report found that attacks on cloud services have more than doubled year-on-year. Ransomware attacks are now the leading form of incident during data breaches as criminals seek to deprive organisations of their critical data.

Businesses are also facing increasing scrutiny from data privacy and security regulations. Following the introduction of the EU General Data Protection Regulation (GDPR) in 2018, there has been a wave of new mandates that grant citizens more control of their personal information and mete out potentially huge fines to organisations that fail to safeguard data in their care.

These factors mean data security continues to be an important business priority. To take stock of how organisations are developing their data security strategies, Trustwave surveyed nearly 1,000 full-time IT professionals around the world with influence or decision-making responsibilities on cyber security. The results shone a light on trends in how data is being both managed and secured, as well as plans and concerns for the future.

One of the most notable trends in data management has been the movement of more sensitive data to the cloud. While in previous years many firms held off of migrating their most sensitive and mission critical information to the cloud, 96 percent of respondents stated they plan to move sensitive data to the cloud over the next two years. Fifty-two percent were planning to move highly sensitive data, up to 57 percent with Australian respondents.

Hybrid cloud strategies are the most popular approach, with just over half of respondents reporting the use of both public cloud and on-premises data storage. Globally, just 18 percent of organisations exclusively used cloud storage.

However, there were some stark differences between different regions. Singaporean respondents were much more likely to use hybrid models at 73 percent, compared with just 45 percent in the US. The public sector also appeared far less willing to embrace the cloud in general, with 39 percent of respondents working in government bodies reporting they solely used on-premise data storage – 11 percent higher than the average.

Alongside the prevalence of hybrid setups, most organisations are using multiple cloud services. An overwhelming 70 percent used between two and four public cloud services, and a minority of 12 percent used five or more. The use of multiple cloud providers is perhaps a sign of the rapidly growing cloud market, which has made it increasingly easy for organisations to expand their cloud infrastructure. Just 18 percent of respondents stated they had either one public cloud service, or none at all.

The last 12 months have seen a number of important developments in data regulation. The US saw the California Consumer Privacy Act (CCPA) come into law, with a stricter follow on, the California Privacy Rights Act (CPRA) coming in 2021. Nations including Brazil and China have also sought to add their own national spin on the GDPR model into the mix.

However, regulatory developments appear to have had a relatively minor impact on how companies are securing their data. A surprising 60 percent of respondents stated regulations like the GDPR and CCPA have not impacted their database security strategies. This may be indicative of a lack of alignment between information technology and other departments, such as legal, that hold responsibility for the enforcement of new data privacy laws such as the right to be forgotten and data subject access requests (DSARs). Organisations not able to adequately respond to requests around the personal data they hold are leaving themselves open to regulatory action and fines. Similarly, in the event of a data breach, firms found not to be compliant with the GDPR or other applicable regulations could face serious fines in addition to the already steep cost of a serious breach.

For those respondents that did change their database security in response to regulatory demands, some of the most common actions included stronger access controls, the wider use of encryption and more judicious patching processes.

As data estates continue to expand into the cloud, most security decision makers are keenly aware of the threat posed by cyber criminals. However, when discussing potential threats, it quickly became apparent the perceptions do not match the reality.

Malware and ransomware were seen as the most prominent threat against data, with 38 percent of respondents listing it as their biggest concern. Around 18 percent saw phishing and social engineering as the lead threat, with application threats, insider threats and privilege escalation making up most of the remaining responses.

However, these concerns were misaligned with the actual threats the respondents had experienced. Phishing and social engineering were the most common issues, experienced by 27 percent of respondents, followed by 25 percent experiencing malware and ransomware.

Attack experiences tended to vary by region, with the UK and Singapore suffering the most phishing and social engineering, and the US and Australia being hit by malware and ransomware. The government sector also reported higher than average incidents of insider threats than private sector respondents.

THE MOST COMMON MALWARE IN CIRCULATION RELIES ON UNPATCHED SOFTWARE APPLICATIONS

Notably, just six percent of respondents listed misconfiguration attacks as their primary security concern. However, misconfigured cloud databases such as AWS S3 buckets are an extremely common cause of data breach incidents. There have been many prominent cases of poorly configured clouds enabling threat actors to freely access and exfiltrate sensitive data without the need for any authentication. Automated tools can quickly sniff out unsecured online databases, making them one of the easiest low-hanging fruit for threat actors to reach. Research has estimated that more than 33-billion records have been exposed in the last two years due to a lack of proper database security configuration, with a combined cost of nearly $5 trillion.

Patching has long been one of the most crucial cyber security activities. Most common malware in circulation relies on unpatched software applications and unsupported operating systems and organisations with poor patching practices make for extremely easy targets.

Pleasingly, a decisive 96 of respondents told us they have patching policies in place. Roughly three quarters said they applied patches within 24 hours of being released by vendors, a very effective approach that greatly minimises the chances of an attacker exploiting a vulnerability. By contrast a small minority stated they often took more than a week or even over a month to apply patches, which leaves a big window open for potential attacks.

However, while patching schedules are generally good, there is room for improvement on how patches are being applied. Nearly three quarters of respondents relied on automatic patching processes,

which is not always the best practice. While automatic updates are generally suitable for devices like workplace laptops, more sophisticated systems such as databases will often benefit from a manual approach. This gives IT teams a crucial opportunity to apply testing, as well as some additional human oversight to ensure everything is secured.

Software patching is not the only area dominated by automated processes, as we found that 89 percent

IT HAS NEVER BEEN EASIER FOR ORGANISATIONS TO COLLECT, CREATE AND STORE DATA

of companies use automation for access management. Commonly automated tasks include applying least privilege policies to ensure access levels do not exceed a user's role and the removal of access credentials when a user changes role or leaves the company. While automation can be very useful in ensuring these crucial tasks are completed, trusting in automation with no human oversight can lead to serious issues. In particular, the IT team should manually confirm the removal of user access to applications also includes databases, as this is often not the case in standard settings. The reliance on automation for these tasks correlates with the low level of concern respondents had for the risk of insider threats and privilege escalation. Unused accounts that retain privileged access are prime targets for compromise by external threat actors.

Serious data breaches can be enormously expensive, with costs including operational shutdowns, investigation and recovery costs, regulatory and legal action, reputational damage and lost business from disaffected customers. Recent research from IBM analysing over 500 breaches found the average cost of these incidents to be $3.86-million – rising to $388-million for the biggest 'mega breaches'.

Despite the huge burden of responsibility this places on security personnel, we found nearly half of companies relied on small teams of just six to 15 members. Companies in the APAC region tended to have the smallest teams, with half of Singaporean respondents running a team of less than 10 people, while companies in the US were the most likely to field teams of 21 people or more. The small team sizes are particularly significant when contrasted with the fact that most of the companies we surveyed had an employee headcount of over 500, and many had more than 1,000.

The prevalence of small security teams is likely due in part to the ongoing skills shortage in the field. As our survey found, this shortage in staff has led to a heavy use of automation for many critical tasks, although this is not always the best approach for areas like database security management.

An increasing number of companies are seeking support from external third parties to gain access to essential skills and advanced security tools. Managed Security Service Providers (MSSPs) are a particularly effective option for organisations to access a wide gamut of skills and technology on a 24/7 basis to deal with both tactical and strategic security needs. Outsourced security resources will play an increasingly important role in helping organisations protect their essential data as both data footprints and the corresponding level of cyber threats continue to grow.

Organisations will also need to ensure their security strategies continue to evolve to accommodate the increased use of the cloud. They must be equipped with the process, tools and expertise to identify and address cloud-based risks, especially in more complex hybrid and multi-cloud environments. As our findings show, there are still many misconceptions around threats and security priorities, so it is particularly important that new data security strategies are based on real, up-to-date threat intelligence ●

Travis Lee, Director of Product Management at Trustwave, is an experienced product marketing and management leader specialised in cybersecurity and managed payments with demonstrated success in leading matrix teams in product marketing, product management and business development roles.

Regulatory developments have had a relatively minor impact on how companies are securing their data