Data-at-rest encryption: at the centre of the security circle

Published on 29 Jan 2019

The past decade has seen unprecedented growth in data creation and management. The products and services that consumers use every day – and the systems businesses, large and small, rely on – all revolve around data. The increasing frequency of high-profile data breaches and hacks should be alarming to anyone, and there's a danger data security could worsen in the coming years.

According to DataAge 2025, a report by IDC and Seagate, by 2025, almost 90% of all data created in the global datasphere will require some level of security, but less than half of it will actually be secured.

Nuanced approach to data security

> Security is a circle, not a line. Every actor involved in the handling and processing of data has responsibility for ensuring its security

The rapid proliferation of embedded systems, IoT, real-time data and AI-powered cognitive systems – as well as new legislation like the European Union's GDPR – means that data security has to be a priority for businesses like never before. With data used, stored and analysed at both the hardware and software level, we need a new and more nuanced approach to data security.

Security is a circle, not a line. Every actor involved in the handling and processing of data has responsibility for ensuring its security. What this means in practice is renewed focus on areas of hardware and software protection that have previously not been top of mind or received large amounts of investment from businesses, with security at the drive level being a prime example.

The importance of data-at-rest encryption

In a world where data is everywhere, businesses need always-on protection. Data-at-rest encryption helps to ensure that data is secure right down to the storage medium in which it is held in a number of ways. Hardware-level encryption, firmware protection for the hard drive, and instant, secure erasing technology allow devices to be retired with minimal risk of data misuse.

A recent report from Thales Data Threat found that data-at-rest security tools can be a great way to help protect your data. However, it's important to note that this must be used in conjunction with other security measures to ensure that those that fraudulently gain access to your key management system can't access your data.

Ensuring drives to be Common Criteria compliant

> One straightforward test any business can do to ensure its storage is as secure as possible is to check whether the drives are Common Criteria compliant

Despite the clear benefits, this kind of encryption lags behind other areas, such as network and endpoint security, in terms of the investment it currently receives. The same Thales Data Threat report found that data-at-rest security was receiving some of the lowest levels of spending increases in 2016 (44%), versus a 62% increase for network and a 56% increase for endpoint security.

One straightforward test any business can do to ensure its storage is as secure as possible is to check whether the drives are Common Criteria compliant. Common Criteria is an international standard for computer security certification, and drives that meet this standard have a foundational level of protection which users can build on.

Providing an additional layer of security

The retail industry has seen a spate of security breaches recently, with several major US brands suffering attacks over the busy Easter weekend this year. As frequent handlers of consumer card information, retailers are particularly vulnerable to attack.

> Data-at-rest encryption could enhance security in these instances, providing an additional layer of security between customer records and the attacker

The advanced threats retailers face can often evade security defences without detection. Such a breach could grant attackers unrestricted access to sensitive information for possibly months – some breaches are known to have been detected only after consumer payment details appeared on the dark web. These types of undetected attacks are highly dangerous for retailers, which are relatively helpless to protect consumer information once their defences have been compromised.

Data-at-rest encryption could significantly enhance security in these instances, providing an

additional layer of security between customer records and the attacker which has the potential to make the stolen data valueless to cyber criminals.

Industries in need of data-at-rest encryption

Healthcare organisations, which hold highly sensitive customer and patient information, have a strong use case for data-at-rest encryption. With the widespread adoption of electronic patient health records, that data is increasingly more vulnerable to attack. Recent research from the American Medical Association and Accenture revealed that 74% of physicians are concerned over future attacks that may compromise patient records.

With the widespread adoption of electronic patient health records, that data is increasingly more vulnerable to attack

The financial sector would also benefit from further investment in data-at-rest encryption, given 78% of financial services firms globally are planning on increasing their spending on critical data,

according to Thales' Data Threat Report.

> It's helpful to view security as a circle in which every piece of hardware and software handling the data plays its part

SMEs and enterprises are not immune to security threats either – with growing numbers of people traveling for work or working remotely, the risk of sensitive business data becoming exposed via device theft is heightened. Usernames and passwords have little use if thieves can simply remove unencrypted hard drives and copy data across.

Securing every hardware and software

Technology vendors often focus on aspects of hardware and application security that are within their control. This is understandable, but it risks proliferating a siloed approach to data security. There is no single line for data security -- rather, it's helpful to view it as a circle in which every piece of hardware and software handling the data plays its part.

There's a clear need for more industry dialogue and collaboration to ensure data security is effectively deployed and connected throughout the security circle and across the value chain.

Author Profile

Andrew Palmer

You may also be interested in...

GDPR, hybrid storage and AI: key physical security trends for 2019

We're here again. The end of another calendar year, and a time when many organisations are assessing their performance over the past 1...

How organisations can secure user credentials from data breaches and p...

In the age of massive data breaches, phishing attacks and password hacks, user credentials are increasingly unsafe. So how can organisations...

New Year's Resolutions to counter web and mobile application security...

With the coming of a New Year, we know these things to be certain: death, taxes, and… security breaches. No doubt, some of you are ma...

Can we prevent active shooters through AI technology?

According to the reports of not-for-profit organisation Gun Violence Archive, the year 2018 has seen 323 mass shooting incidents as of Novem...