Reducing risk

With cyber-attacks now inevitable and data breaches highly likely, it is logical that companies should evaluate their investment in security by their ability to reduce risk.

Enterprises face an overabundance of different types of risk, including business, operational, market, and systemic risks. The evolution of connectivity generally, and e-business in particular, have brought with them an ever-present threat of cyber-attacks, and cyber-risk has joined the range of risks to be factored into the cost of doing business.

With cyber-attacks now inevitable and data breaches highly likely, it is logical that companies should evaluate their investment in security by their ability to reduce risk.

Investments in the many forms of end point and network security continue to grow rapidly. Identity management technology is growing at a slower pace but is still a well-established, multibillion business. A third area of activity, namely data security, is by comparison relatively neglected.

Data security is better at risk mitigation

Breaches are not if, but when

It has become something of a fact that, in the current state of cybersecurity, being breached has become a question of when, not if, for organisations. As a result, security vendors have shifted their focus from prevention to detection and response, which initially means mitigation, then remediation. This change, while it represents an acceptance of the new reality, is also an admission of defeat.

As a consequence of this scenario, organisations now include cyber as one of the many types of risk that they must manage, alongside commercial, financial, systematic, or market-wide risk.

Data security reduces risk

In the digital age more than ever before, data constitutes the crown jewels of every enterprise, and it is precisely what cybercriminals are after when they penetrate a corporate infrastructure. In this context, data security is a vital ingredient in any enterprise risk-management strategy, with investments in data security correlate directly to risk mitigation.

The increasing overlap of compliance and security as it relates to data is key to why data security reduces risk more effectively than security provisions for the end point or network.

Investments in breach reduction are a necessary part of cybersecurity spending, while maintaining an up-to-date infrastructure for identity is a key part of digital transformation. End point and network security are both extremely important. However, the return on investment in data security, in terms of both improved security posture and risk reduction, is both more immediate and unparalleled in its efficacy.

Data breaches represent direct costs, in terms of the time and resources spent communicating with customers, possible monetary settlements of lawsuits, and – depending on the sector – fines paid to authorities. In addition, there are the indirect costs of lost business and customers, the so-called reputation hit (with a knock-on effect on a public company's share price) and, of course, loss of market share.

Compliance is a further driver for data security

Compliance requirements, most notably the European Union's General Data Protection Regulation that came into force in May 2018, have brought increased attention to data privacy and the need not only for more controls on data movement, residency, and access, but also for better security practices.

The increasing overlap of compliance and security as it relates to data is key to why data security reduces risk more effectively than security provisions for the end point or network. Database security is a key component within data security, so let us now turn to that area of technology.

Database security has operational benefits

Database security can have significant operational benefits. It can, for instance, uncover unknown, rogue, and even simply disused databases within an organisation's infrastructure, making it possible for them to be shut down, thereby reducing the corporate attack surface.

It also identifies all the places where a company's most sensitive data resides, helping focus the mind of corporate defenders on where they need to concentrate their efforts. To quote the old IT security aphorism, "You can't protect what you can't see."

Blue Cube Security reports

There is no doubt that continued investment in end point and network security, is a worthwhile endeavour, and indeed, new forms of protection are continually emerging to enhance this area of security.

Using database security, companies can gain visibility into who is accessing data, when it is being accessed, and how it is being used. Companies can also pinpoint critical threats to critical data by applying machine learning and security analytics, which also allows security teams to better address the problems raised by event overload and alert fatigue.

Aside from the obvious contribution this makes to mitigating risks to confidentiality and integrity and reducing the threat of external and internal data theft, the increased visibility can identify gaps in the company's IAM process, such as excessive rights or the existence of dormant accounts, thereby helping to fix IAM. As such, it can also be seen as enhancing the operation of core security (i.e., identity services), in that it provides a clear picture of who is doing what, when, and how.

And, of course, the effective use of database security has a key role to play in helping companies comply with the multiple data privacy and security regulations now in place or about to be introduced around the globe.

Recommendations

Think data security first

In formulating security policy, begin by focusing on risk. Data security can reduce risk in a more effective manner and should be prioritised when you are defining your security posture. Once you have got data security right, then you can decide what to do in end point and network security.

Data security is a key differentiator in the data-driven world

If done right, data security can enable an organisation's business growth without constraining the flow of data.

Security goes beyond .....

There is no doubt that continued investment in end point and network security, is a worthwhile endeavour, and indeed, new forms of protection are continually emerging to enhance this area of security. Equally, the way you deliver identity services, particularly to employees and business partners/contractors, can now benefit from the ubiquity and facility of cloud computing. However, in order to reduce risk, securing your critical data should be your first priority, with end point and network security serving as additional layers to be built around data security. □