How to get the most out of your security investment

15/04/2016

In today's digital age, ensuring your organisation's sensitive data remains secure within company walls goes far beyond simply buying and implementing a security solution. With the elevated threat of increasingly sophisticated cyberattacks, it is absolutely necessary that companies understand which security solution best fits their IT environment and what steps need to be taken in order to ensure they are getting a continual return on their investment.

All too often organisations look to resolve security issues by simply purchasing more expensive security products, without ensuring the solution can evolve with the company. However, misconfigured or poorly set up security tools do not offer increased security, rather, they can lead to increased vulnerability.

SEE ALSO: An early guide to the UK's best 4G LTE: EE vs Vodafone vs O2 vs Three

Build a long-term plan for your security investment

The proper implementation, configuration and use of data security tools start with planning. All organisations should have a detailed plan that outlines security software objectives, the solutions that are currently in use (or the criteria for choosing a future solution), workflows, tasks with owners and clear steps for auditing. With no guidelines, security investments can be made without understanding the long term strategy.

Data security handled by the IT department or, in smaller companies, by an IT admin, should be treated like any other part of the business. If the finance department contributes to tracking expenses and revenues and seeks to optimise profit, the IT security protects intellectual property and makes sure business is not affected by downtime and other consequences of a data breach. So, in addition to having clear guidelines, the IT department should be aware of its role in the organisation and its importance for business continuity.

Find the best security solution for your company

Once this is settled, the CISO or IT admin needs to make sure they implement data security tools that cover all vulnerabilities, or at least the biggest ones, and that they do not have conflicts with security solutions already installed. These days, threats come from every connected channel including portable storage devices, insider error, cloud apps, mobile/wearable devices, IoT, and more.

If there are dependencies between security tools your company uses, or the tools can be somehow integrated, it is recommended to make sure they work properly and do not cause problems like high resource consumption or system crashes. Above all, the solution to securing your company's data is not to purchase more expensive security products, but to value the technical aspects of vendors' services like support, which is extremely important in case of a breach or system failure, product roadmap and vision for future improvements.

Continue to analyse and improve

After implementation and configuration, it is very important to continue analysing and improving upon the software you have deployed. Every day security products need to be improved and updated, not only by the vendor, but also by the enterprises to adapt to new threats. The solutions must allow the CSO to focus on new threats from high to very low level.

When it comes to day-to-day data security updates, including changes in policies, incident response, etc., it is up to the IT manager or CISO to initiate and follow-up to ensure they are done properly. The main challenges – or better said, pitfalls – that lead to security incidents are often related to the IT department's team or manager:

- Ignoring the guidelines
- Superficially evaluating the data security software
- Ignoring the vendor's best practices or administration guides or failing to communicate with the vendor if they find issues or bugs
- Disregarding the security patches or feature updates
- Rejecting the renewal of the software, thinking that they do not need support or updates
- Skipping the audit

The key is to give ownership for each security related task and hold each team member and manager responsible for what's going on.

How to respond to a security breach: Plan,do, check, act

In an ideal world, every security executive should be up to date, invest in the right solutions and have risk management in place to avoid getting hacked. But until we get there, organisations need to arm themselves with an appropriate response.

We spoke with Erdal Ozkaya, an IT security guru and CISO at EMT Distribution, for his recommendations on the immediate first steps any company or executive should take in the case of a security breach:

Let go of your ego

If a security breach is too complicated for the onsite team, the internal security expert should work with professionals (such as Incident Response Teams) who can understand if the breach is still active or not.

Figure out what went wrong

It's a good idea to do a Forensic Analysis to find out what went wrong and what was changed and more importantly what data might have been exposed.

Eliminate the problem

After all this, make sure the problem is eliminated, patch the systems, change the passwords, run a vulnerability assessment and implement a Risk Management strategy and rebuild the environment based on learned lessons.

Invest in training

Everyone in an organisation should be trained against possible phishing or Social Engineering attacks.

Test, test, test

Security executives must make sure they conduct a regular simulated network attack (penetration testing) against their organisation, so basically hack themselves to find out their weaknesses, check them, act on them. It all comes down to 4 steps: 'Plan, Do, Check, and Act' which represent a continuous process which will NEVER stop.

Erdal has found that Data Loss Prevention solutions (DLP) offer valuable information if breaches occur, which normally doesn't happen if policies are properly built. The available reports provide details like confidential data transfers that took place, from which computers, at what time and the exact transferred content. Once IT Administrators or security staff analyse these reports, they can address the issue by restricting data transfers for the problematic users, they can even use the reports as proof in court or they can take further measures depending on the vulnerability.

Roman Foeckl is the Founder and CEO of CoSoSys