Roman Foeckl

The 4 Biggest Mistakes Businesses Make Trying To Secure Endpoints

Sure, it's tempting to chase whatever collaboration technology is hot at the moment, but this can cause serious data security risks.

To increase productivity and attract the best talent, many companies encourage employees to take advantage of the latest and greatest advancements in collaborative technology. However, many fail to take into consideration the risks this causes. Corporate data becomes vulnerable and difficult to protect, and infrastructure becomes increasingly complicated because of the many devices and other endpoints that connect to the network. All devices, smartphones, tablets, laptops, computers, servers, USB keys, and other technologies that are part of the same network are endpoints.

It's not enough anymore to protect endpoints from malware; external threats have become more sophisticated because attackers are using creative methods to penetrate organizations' networks. Moreover, insider threats are becoming more powerful, with employees editing or sharing highly sensitive data (such as documents that contain confidential information) without being aware of the consequences. A data breach or loss of confidential information can shut down the business.

Not giving enough importance to data security is one of the main reasons some businesses fail to protect their data. It's not enough anymore to protect endpoints from malware; external threats have become more sophisticated because attackers are using creative methods to penetrate organizations' networks. Moreover, insider threats are becoming more powerful, with employees editing or sharing highly sensitive data (such as documents that contain confidential information) without being aware of the consequences. A data breach or loss of confidential information can shut down the business. That's why it's important to avoid these four common mistakes:

1. Underestimating Human Error: This is the most common mistake I see. The IT manager or CSO treats external threats as a high priority but disregards human error. This leaves a big gap in data security because bad employee habits (bringing their own mobile devices to work, downloading unsanctioned apps, circumventing the security policies, and ignoring that sensitive data shouldn't be shared on unapproved apps or devices) will get worse if they aren't addressed. The tools and apps employees need to perform their jobs should be important elements in every data security plan. This way, when selecting data security solutions, the chances of aligning the IT department's needs with employees' needs are greater.

2. Passing all Responsibility to the IT Department: The interest that top management and business unit managers have in data security plays a big role in the success of protecting the company's data. Many organizations don't think of data security as an ongoing business problem, don't include it in their business goals and budget, or they just pass it to the IT department. These organizations aren't aware of the big negative impact a data breach could have for the business, its clients, partners, and other stakeholders.

Others invest a lot of resources in security, but they manage them poorly. They acquire many IT security tools and let the IT department figure out their purpose and how to optimize implementation. The responsibility and proportion of the data protection program are far too big to be left only in the IT department's hands.

3. Superficial Protection: Setting up an antivirus solution and a firewall is often close to doing nothing. It's a superficial way of securing data because the old days, when malware was the main concern, are long gone. Threats have evolved and so have data protection solutions. Another mistake many organizations make is to skip updating their security systems. By doing this, they don't take advantage of the feature and maintenance updates that vendors release, failing to address the newest threats. Treating the data security problems superficially is sometimes worse than not treating them all.

A classic error in the data loss prevention sector is to purchase DLP solutions and then create irrelevant policies, either because confidential data isn't properly defined, the level of authorization and exceptions are misconfigured, or the entities aren't clearly defined. For example, it's easy to make mistakes when setting up policies when there are networks with the same computer name for all computers, even when the computers can be uniquely identified by IP or MAC address.

4. Thinking That Compliance Is the Same as Security: For businesses, sensitive information that can be lost or stolen includes financial information, intellectual property, Social Security numbers, credit card numbers, and other business records. In the last few years, a lot of progress has been made in developing rules and regulations to standardize data security implementations. There are multiple regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI-DSS), that organizations need to comply with in order to avoid fines and penalties. Achieving compliance with these rules is a must, but one of the biggest mistakes that companies make is to purchase security solutions and either keep them on the shelf and deploy them in case of an audit, or install them but use just the basic features, again, to be covered in case of an audit.

Sometimes, organizations need to stop and see what they're doing wrong to be able to rethink their next steps and restructure their data security plan. First, they need to stop underestimating human error and start educating their employees about data security. Next, they need to make data security a business problem. And finally, they need to stop treating data security superficially and reject the notion that compliance equals security.

Roman Foeckl leads CoSoSys. The company is a leading developer of mobile device management (MDM), data loss prevention (DLP), device control, network endpoint security, and portable storage encryption solutions for Windows, Mac OS X, and Linux. It has ...