Secure
Protect
Comply

Hackers Aren't Your **Biggest Threat**

CYBER INSIGHTS

CTG Managed Cyber Security

The state of information security for companies in the U.S. is scary. 2014 was a record setting year in terms of data breaches with a staggering 783 breaches reported. That means on average more than 2 breaches were reported every day in 2014. The percentage by industry sector remained about the same as previous years although Health and Medical have the lion share at 42.5% and Business at 33%. When people hear about breaches, they immediately think about hackers. Yet hacking is responsible for only 29% of breaches. The other 71% of breaches are in incident category types such as insider theft, data on the move, accidental exposure, subcontractors, employee negligence and physical theft. These less focused on causes of data breaches are just as damaging to an organization as a hacker attack. In fact in many cases they are more damaging. For example, most people have a general belief that hackers are so good that if they want to compromise a company or system, they can. So when a business is compromised by a hacker, many people say, "well there isn't much you can do about those bad guys". Yet, when an employee sells information on the black market or a 3rdparty contractor exposes information or a server is stolen from an office, people immediately assume that the company could have done more to prevent it. This can have deep and lasting impacts on the reputation of a company, the revenue and profits, lawsuits, regulatory compliance impacts, fees, etc. For large companies it can impact stock prices and invoke executive management changes. For small companies, it can trigger the need to sell or merge with another company at fire sale prices, or can lead to simply going out of business.

Insider Theft

Breaches that come from employees are often the most damaging. More than 10% of all breaches are caused by insider theft. Any size company may deal with this. In 2014 alone insiders caused breaches at large companies such as Capital One, VAMC – San Antonio, and Home Depot as well as small organizations such as the Western Regional Center for Brain and Spine Surgery, Ladies First Choice, Inc. and University of Massachusetts Memorial Medical Center. In some cases, new loans and accounts were opened in others names. In other cases the information was sold. Some is due to disgruntled employees. Other times it may be because employees release information to the media because they don't believe the company is being honest, ethical, or doing the right thing.

First, organizations should always limit access rights to only those individuals whose job requires access to sensitive information. Unfortunately access rights are often given for being in a particular active directory (AD) group. Additionally, the IT folks in an organization usually have unlimited rights and can grant any rights they wish to others. Other times executives and other influential employees can simply request permissions to directories or databases and can subvert the standard access control process. In small organizations, most everyone is trust and therefore given permission to sensitive data whether they need it or not..

Subcontractor

3rd parties and subcontractors in 2014 represent more than 15% of all data breaches. This is the second most common breach after hackers. These are individuals or companies that have access to your sensitive data. It can be 3rd party billing and payment processors, external IT folks, maintenance workers (like the HVAC contractor that ultimately led to the Target breach), or just about anyone else. Some 3rd parties need access to sensitive data. Most do not. Yet many have access to either physical equipment that stores sensitive information or system access to data.

Where so many companies are now beginning to use and store sensitive data on cloud service providers it opens up a whole new level of exposure. Most companies don't realize that when they place their data with a hosting provider, cloud provider, etc. they are giving access to those companies and anyone they allow to your data. Yet the benefits of using the cloud are so great that we can't digress and continue in a client/server environment which has many risks of its own.

Employee Neglegence

Negligence by an insider consists of a broad range of possible events and circumstances. Employee negligence was almost 11% of all data breaches in 2014. Primarily training and testing of employees is the best way to reduce the risk of insider negligence, however some solutions are effective at reducing the risk of employee negligence by limited access to only those users that need to access sensitive data.

Physical Theft

Burglary is primarily responsible for the entire physical theft category of breaches. It constitutes 12.5% of data breaches in 2014. This is a huge risk for small and medium sized businesses, especially those that still house their own servers and databases in their offices. Unfortunately, often the thieves are stealing the equipment simply to sell and they don't care about the data. However, losing control of the data in most states constitutes a data breach that must be publically disclosed, especially if that data is not encrypted.

Solution

Solutions that can mitigate the risk of some of these other incident types including insiders and 3rd parties are not nearly as prevalent as those an organization can implement to prevent hackers. Yet it is far more likely that you will experience one of these non-hacker related. The answer is a unique combination of encryption, access controls and auditing that is completely transparent to users and will dramatically reduce your organization's exposure to these non-hacker breach sources.

How it works

With agents placed on each server storing sensitive data, encryption keys are issued from your provider. The agents communicate to the key management servers which instruct the agent which data to encrypt and who can have access to it. The agent then controls the encryption and decryption of data in real-time. The access controls are separate from your internal AD which allows more granular control and can block those administrators and IT personnel that normally have access to everything. Auditing and reporting can be enabled so you can see who is accessing what and when they are doing it. This allows you greater insight into malicious activity by insiders and may even help detect when hackers are using an insiders authorized credentials to access sensitive data. This reduces the time to discovery and mitigation.

This solution works regardless of where your servers and data is located. If it is hosted at a cloud provider, the provider would only have access to encrypted data without any access to the keys to decrypt it. This keeps your data secure from hosting providers and other 3rd parties.

No software or configuration is needed on the employees' endpoint systems and all applications work as they normally would. It is completely transparent to users and other systems that interact with your sensitive data.

Your provider hosts the encryption keys but doesn't have any access to your data, which is another added layer of protection for your organization. By separating the key management from where the data is located, your organization is much more protected from these common breach types. Insiders are limited to only those that need access to the data and IT folks are prohibited for accessing the data unless otherwise authorized. Subcontractors don't have access (unless authorized) and even hosting and cloud providers only have access to secure encrypted data. The chance of employee negligence is reduced due to separated access controls where users are not inadvertently added to groups or given default permissions to data they should have access to. Physical theft of your servers and databases where sensitive data is stored is no longer an issue. The data is encrypted and if stolen, the thieves cannot view or use your data. In fact in the vast majority of states, you don't even have to report this type of data breach if your data was encrypted when stolen because the information cannot be used.

Conclusion

An encryption solution is one of the few technologies available today that can reduce the risk to these often overlooked breach sources including insiders (both malicious and negligent), 3rd parties, and physical theft (unless you are the victim of such a breach). While doing your next business risk assessment, make sure you are considering all breach types. Then compare the overall impact of a breach to what is a comparatively minor cost to deploy a solution that has the power to mitigate such a large part of your business risk landscape. To find out more, visit us at https://www.ctg-managedit.com .