cyber.calian.com

ISSUE
#14

THE BREACH REPORT

Gunnebo AB

CYBER SECURITY SOLUTIONS

CALIAN®

cyber.calian.com

The Background

In today's digital business environment, enhanced and holistic cyber security is essential. However, many companies continue to struggle with resilience, often experiencing breaches that lead to everything from compliance issues, to lost and stolen data and, ultimately, to brand damage and revenue loss. And though it is easy to read about these breaches, the causes and potential solutions are rarely identified.

It is for these reasons that Calian has created the Breach Report. Each month, we spotlight a particular type of company, the breach it has experienced, and what it could have done to mitigate risk against the specific type of cyber attack—all to create better insight for the general public and to educate people on proper cyber security best practices.

In this month's report, we spotlight a ransomware attack that struck Sweden’s leading multinational security firm, Gunnebo.

cyber.calian.com

The Company Profile

Gunnebo is a global provider of security products, services and software to control the flow of valuables, cash and people. It offers entrance control, safe storage, cash management and integrated security solutions to customers primarily in banking, retail, mass transit, public and commercial buildings, and industry and high-risk sites. The company has operations in 25 countries, more than 4,000 employees, and billions in revenue annually.

CYBER SECURITY SOLUTIONS

CALIAN®

cyber.calian.com

The Environment

In August 2020, after Gunnebo refused to pay a ransom, the Mount Locker ransomware group uploaded 18Gb of sensitive customer data - the equivalent of about 38,000 files - to a public server on the dark web.

The Outcome

The stolen data includes information about ATMs security functions, drawings of client bank vaults, and alarm and monitoring equipment. This also includes data and confidential blueprints from Sweden's national legislation, the country's supreme decision-maker Riksdag, and the Swedish Tax Agency.

According to Hackread.com, it is possible the stolen data is also circulating on different hacking forums through the MEGA download link.

The Potential Risk

While the hack took place some months ago, its effects only recently came to light in late October 2020. To date, Gunnebo has downplayed the impact of this substantial breach. However, it is believed that many of the stolen documents are confidential security blueprints from at least two German banks, Sweden's national legislation, the country's supreme decision-maker Riksdag, and the Swedish Tax Agency.

In addition to potential risk to customers, Gunnebo is also facing a serious risk to its reputation. According to TechRadar.com, it is thought that hackers gained access to Gunnebo's network by stealing the credentials of a remote desktop protocol account. "It has also been revealed that the stolen password in question was 'password01' - an embarrassing disclosure for any company, but particularly one working in the security industry."

The Solution

As data breaches continue at alarming rates, securing sensitive data is critical to all organizations. Implementing a proper data security platform can greatly reduce risk by integrating data discovery, classification, data protection and more granular access controls, as well as enabling centralized key management.

Key management

An enterprise key management solution enables organizations to centrally manage encryption keys, provide granular access controls and configure security policies. It also manages key lifecycle tasks including generation, rotation, destruction, import and export, provides role-based access control to keys and policies, and supports auditing and reporting.

Data discovery and classification

This type of solution locates regulated data, both structured and unstructured, across the cloud, big data and traditional data stores. A single pane of glass delivers understanding of sensitive data and its risks, enabling better decisions about closing security gaps, compliance violations and prioritizing remediation. A data discovery and classification solution also provides a streamlined workflow all the way from policy configuration, discovery and classification, to risk analysis and reporting, helping to eliminate security blind spots and complexities.

Data-at-rest encryption

Data-at-rest encryption delivers privileged user access controls and detailed data access audit logging. Agents using this kind of solution should protect data in files, volumes and databases on Windows, AIX and Linux OS's across physical and virtual servers in cloud and big data environments.

Application data protection

Application data protection delivers crypto functions such as key management, signing, hashing and encryption services through APIs, so that developers can easily secure data at the application server or big data node. This solution also enforces strong separation of duties through key management policies that are managed only by security operations.

Tokenization

Tokenization replaces sensitive data with a representative token, so that the sensitive data is kept separate and secure from the database and unauthorized users and systems.

Database protection

Database protection solutions integrate data encryption for sensitive fields in databases with secure, centralized key management and without the need to alter database applications. This kind of solution should support Oracle, Microsoft SQL Server, IBM DB2 and Teradata databases.

References

Ballard, Barclay (2020, October 29). Nuclear power stations, airports at risk after hackers breach security giant. Retrieved from https://www.techradar.com/news/nuclear-power-stations-airports-at-risk-after-hackers-breach-security-giant/

Waqas (2020, October 21). Mount Locker ransomware group leaks 18Gb worth Gunnebo AB data. Retrieved from https://www.hackread.com/ransomware-group-donates-20000-in-btc-charities/

CALIAN®

CYBER SECURITY SOLUTIONS

Contact us for a **free consultation or to receive a free Cloud Security Audit** to assess the effectiveness of your current cyber security initiatives.

1.877.225.4264

www.calian.com

THE BREACH REPORT