cyber.calian.com

ISSUE
#15

THE BREACH REPORT

DATA BREACHES IN ONLINE EDUCATION

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 widespread attack that struck five e-learning websites around the world earlier this year.

cyber.calian.com

THE COMPANY PROFILE

In October 2020, the WizCase hactivist team reported they had discovered multiple data leaks of almost 1 million records from five separate e-learning companies. The companies included:

- Escola Digital (Brazil)—a website offering a wide range of digital courses for students and teachers
- MyTopDog (South Africa)—e-learning for grades 4-12, providing personalized learning experiences
- Okoo (Kazakhstan)—an online learning platform for children
- Square Panda (US)— a multisensory edtech phonics literacy platform for pre-readers and early readers
- Playground Sessions (US)—a virtual piano lesson platform

THE ENVIRONMENT

These companies had stored the exposed data in misconfigured and unencrypted Amazon S3 buckets, as well as an ElasticSearch server.

The result was that anyone without any form of authentication could access personal identifiable information including full names, cellphone numbers, passwords, email addresses, dates of birth, gender, guardian information, completed courses, lessons, test scores and more.

Altogether, these five breaches involved almost 1 million user accounts, with some accounts dating back as far as a decade.

Almost all the stolen data pertained to children under the age of 18.

cyber.calian.com

THE OUTCOME

- **Escola Digital**—Nearly 75,000 active user accounts between 2016 and 2017 were breached. On top of personal identifiable information, the misconfigured bucket included links to certificates of users who attended the platform's online classes.
- **MyTopDog**—Exposed personal identifiable information of 800,000 student records via a misconfigured Amazon S3 bucket, with some records dating back to 2016-17.
- **Okoo**—Exposed 7,200 user records through a misconfigured 418 MB database, plus approximately 1 million entries about user activity on the platforms and analytics. In addition to student information, admin credentials were also hacked.
- **Square Panda**—Almost 15,000 user accounts were breached through a MB CVS file, which stored a backup of users' personal data.
- **Playground Sessions**—Revealed the private information of about 4,100 users registered from 2011-13.

cyber.calian.com

THE POTENTIAL RISK

Due to the ongoing pandemic and COVID-related school closures around the world, there has been a recent surge in the global usage of e-learning platforms.

Many users whose data was leaked are no longer active on the affected websites. Many also will be unaware that those companies still have their information.

Regardless, the affected platforms are used predominantly by children. Companies dealing with personal information pertaining to minors must make young people's data protection their utmost priority. It is crucial to take measures to ensure such data does not get into the wrong hands—which could be used to commit any number of crimes like identity theft, fraud, stalking, blackmailing, and phishing scams.

THE SOLUTION

The most important exercise an organization can take part in is a comprehensive Penetration Test.

This kind of test will enable a determination of the current state of exposure and the steps that can be taken to build cyber resilience.

More so, the right advisory services also deliver a framework that sets out a roadmap for a cybersecurity program.

Cybersecurity Risk Assessments
These in-depth assessments of an organization's controls and maturity based on industry security standards and regulations should be a priority. Assessments can include threat risk assessments, enterprise maturity assessments, and enterprise readiness assessments against ransomware and other advanced persistent threats.

Industry security standards should include:
- NIST SP series
- ISO 27001/27002
- IEC 62443 series (for industrial control systems)

Regulations should include:
- PCI-DSS
- PHIPA
- PIPEDA
- PCI-DSS

Penetration Testing

Ethical hackers fully scrutinize the environment while attempting to breach data. Testing scenarios include red team and purple team exercises against:

- Applications, infrastructure and network
- Operating system and database
- Wireless networks

Cloud Security Assessment

Often, cloud environments are gradually built without overarching security frameworks and standards to support their configuration. Unfortunately, this can lead to insecure setups and exposure to attacks.

Cloud Security Assessments review the security configuration of services such as Microsoft Azure, Amazon Web Services (AWS), Google Cloud Platform (GCP) or Microsoft Office 365 environments to provide actionable risk-based recommendations.

Industry best practices should include:

- Centre for Internet Security (CIS) benchmark

References

Bizga, Alina (2020, July 21). Cybersecurity Researchers Discover 5 e-Learning Websites Leaking Nearly 1 Million User Records. Retrieved from https://securityboulevard.com/2020/07/cybersecurity-researchers-discover-5-e-learning-websites-leaking-nearly-1-million-user-records/.

Cisomag (2020, July 20). E-Learning Platforms Continue to Suffer Data Breaches; 1 Mn Records Exposed. Retrieved from https://cisomag.eccouncil.org/data-breaches-on-e-learning-platforms/.

Williams, Chase (2020, October 2). Data Leaks in Online Education: Almost 1 Million Records Exposed. Retrieved from https://www.wizcase.com/blog/educational-breaches-research/.

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