CALIAN®

THE BREACH REPORT

ISSUE #7

www.calian.com
1.877.225.4264 | 770 Palladium Drive, Ottawa, ON, K2V 1C8

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 an alarming exposure: In total, 250 million Microsoft customer service records were exposed for most of December 2019 (Winder, 2020).

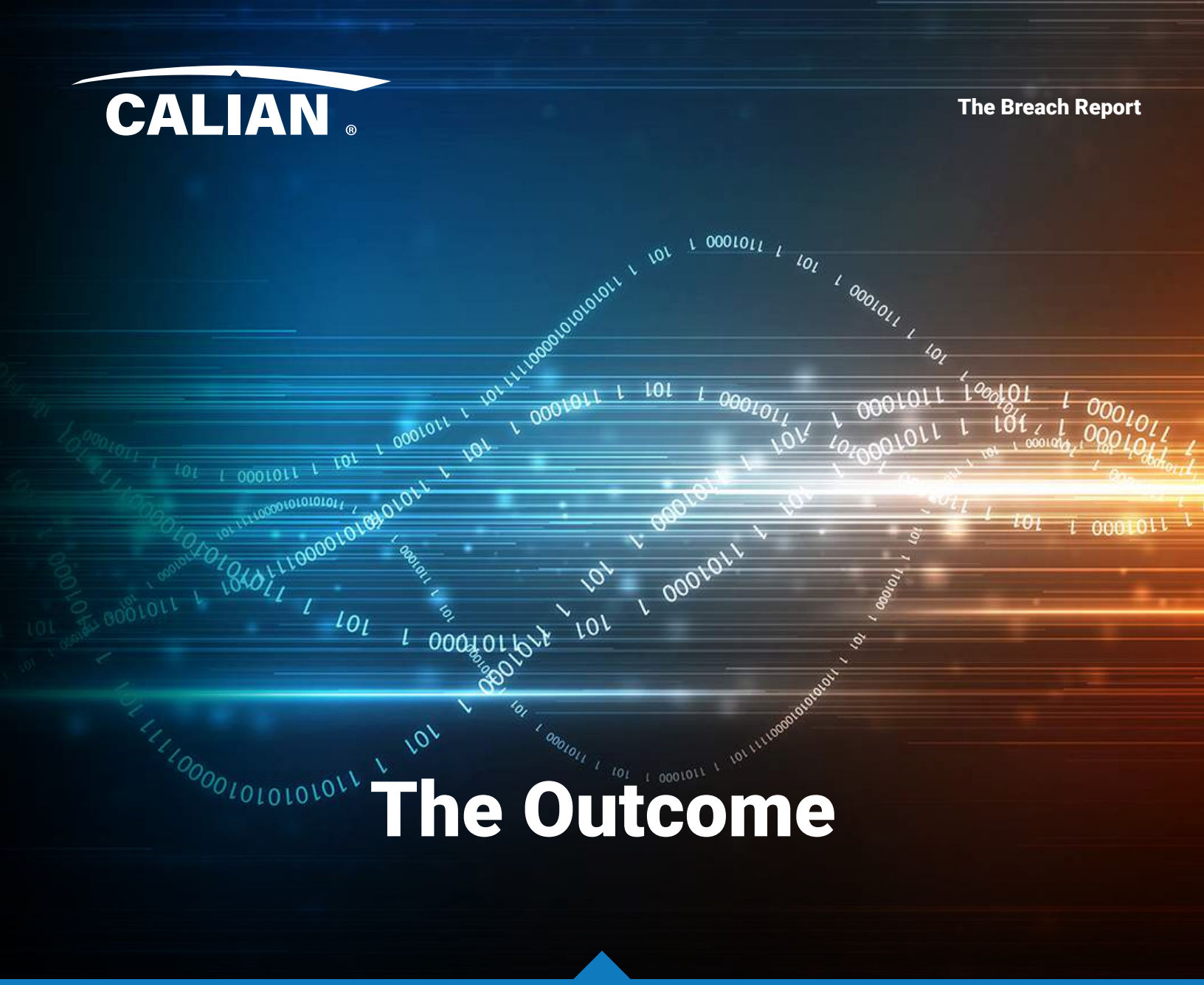
The Company Profile

Microsoft revealed that it uncovered misconfigured security rules in a database on December 29, 2019. It was an internal company database used for analytics, apparently not normally accessible to the outside world (MSRC Team, 2020).

Microsoft has continuing security issues. Early in 2020 the company had to push an emergency security update to all users after the NSA found a critical vulnerability in its cryptographic systems. And then, just a few days later, a serious vulnerability was discovered in Internet Explorer that the company had not opted to patch despite declaring ongoing support for the browser for at least the rest of the active life of Windows 10 (Ikeda, 2020).

The Environment

The 250 million Microsoft customer service records date back as far as 2005 and are as recent as December 2019, and consist of online chat records between customers and Microsoft support personnel. Microsoft says that personal information was scrubbed from the customer service records before they were stored, but they did at minimum contain email and IP addresses stored in plain text. Security researchers believe that the exposure goes beyond that (Ikeda, 2020).



The Outcome

The issue was fixed on December 31, 2019. After conducting an internal investigation, Microsoft claimed that there was no sign of malicious use, nor did most of the customer service records contain personal identifiable information. Even so, Microsoft did admit that some email addresses entered in non-standard formats might have survived the automatic scrubbing of the logs and have remained in plaintext. Because of this, the company is notifying anyone whose email address was exposed in this way.

In light of this massive exposure, Microsoft has instituted some security policy revisions and will be auditing its internal security policies and putting additional tools in place to ensure that stored customer service records of this type have all sensitive personal information redacted from them. In addition, Microsoft is implementing a new internal alert system to better monitor misconfigurations that can lead to potential breaches.

The Potential Risk

For Microsoft, the primary danger is that their customers' information could be used in technical support scams. Frequently, scammers identify themselves as Microsoft support agents, cold-calling customers to convince them that something is wrong with their computer.

The most common scam is to try to sell the customer an overpriced piece of unnecessary "virus scanning" software—and potentially steal their credit card number in the process. But the bolder scammers may attempt to get the customer to grant them remote control of their computer. Scammers might also simply email customers and try to get them to visit malware links under the ruse of providing some sort of technical support. It is recommended that the victims of this type of breach watch out for fake notifications from scammers who try to impersonate the Microsoft support team.

The cost of such scams is high, and not just financially. In the 2014 Global Fraud Study, survey participants estimated that the typical organization lost 5% of revenues each year to fraud. In the study, it was also estimated that the median loss caused by such scams is $145,000, with 22% of the cases involving losses of at least $1 million. At the time of the survey, 58% of the victim organizations had not recovered any of their losses due to fraud, and only 14% had made a full recovery. The damage caused to an organization's reputation lasts months, if not years (ACFE, n.d.).

The Solution

Data protection has always been an object of serious attention by enterprise security executives and compliance officers, but the recent privacy laws will undoubtedly elevate data protection to the boardroom due to the potentially serious consequences of noncompliance. What makes it even more challenging is that companies of all sizes are adopting cloud-based services, such as Microsoft Office 365, to give their employees greater flexibility and easier access to core business applications.

As regulations and corporate needs place increasing demands on IT to ensure safe data handling, deploying necessary protective solutions can seem daunting. Some data loss prevention (DLP) products require substantial efforts to deploy and typically have large ongoing consulting costs. Some DLP products leave it up to IT to know about all the data that needs to be protected, adding an administrative burden and causing false positives. Others rely on the IT administrator to manage disparate consoles across multiple environments—endpoints, network, and the cloud. When are "good enough" products not good enough?

Why DLP?

DLP products enable companies to:

- **Protect Data Where it Lives** – DLP safeguards intellectual property and ensures compliance by protecting sensitive data on premises, in the cloud, and at endpoints.
- **Remain Compliant** – Prioritizes the remediation of critical compliance information and highly sensitive data over less critical data.
- **Enable Centralized Incident Management and Reporting** – Manages all DLP violations and reporting regardless of whether the violations are coming from corporate devices or cloud applications.
- **Synchronize On-Premises and Cloud DLP Policies** – Leverages a common policy engine across endpoints, networks, and the cloud. There's no need to recreate policies to protect the same data in different environments.
- **Gain Visibility** – Capture technology shows how the data is being used and how it is leaking.
- **Quickly Identify Data** – Stronger data classification identifies and classifies data that is important to the organization.
- **Remediate Policy Violations** – Encrypts, redirects, quarantines, or blocks data transmissions that are in violation of policies.

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

CALIAN®

References

Winder, Davey (2020, January 22). *Microsoft Security Shocker As 250 Million Customer Records Exposed Online*. Retrieved from https://www.forbes.com/sites/daveywinder/2020/01/22/microsoft-security-shocker-as-250-million-customer-records-exposed-online/#8bf10654d1b3

Microsoft Security Response Center (MSRC) (2020, January 22). *Access Misconfiguration for Customer Support Database.* Retrieved from https://msrc-blog.microsoft.com/2020/01/22/access-misconfiguration-for-customer-support-database/

Ikeda, Scott (2020, February 3). *250 Million Microsoft Customer Service Records Exposed; Exactly How Bad Was It*? Retrieved from https://www.cpomagazine.com/cyber-security/250-million-microsoft-customer-service-records-exposed-exactly-how-bad-was-it/

ACFE (n.d.). *Report to the Nations on Occupational Fraud and Abuse. 2014 Global Fraud Study*. Retrieved from https://www.acfe.com/rttn-summary.aspx

THE BREACH REPORT

ISSUE #7

CALIAN®

www.calian.com

1.877.225.4264 | 770 Palladium Drive, Ottawa, ON, K2V 1C8