CybelAngel

Identify and Remediate Data Leaks across the Supply Chain

WWW.CYBELANGEL.COM

Identify and Remediate Data Leaks across the Supply Chain

SUMMARY

Data leaks happen, but data breaches and abuse can be avoided. CybelAngel, a global provider of digital risk management services, helps companies detect and remediate data leaks. CybelAngel identifies internal data leaks, plus external data leaks, such as those that occur in the Supply Chain.

Surviving the Service Provider Security Breach

German media cover data breaches nearly every day. A significant data breach occurred in August 2019, when it became public that data from the bonus program "Mastercard Priceless Specials" had been tapped from a service provider's platform.[1] This data breach involved about 90,000 records, including names, email addresses, addresses, dates of birth, telephone numbers, and partly encrypted credit card numbers. In addition, another list of complete credit card numbers circulated on the internet.

If there is unauthorized disclosure and misuse of personal data, the breach of data protection must be reported to the competent supervisory authority, as stated in the European General Data Protection Regulation (GDPR). The notification period is only 72 hours after the data protection violation has become known to the company concerned.

If the data leak occurs at a service provider, as it did with the Mastercard bonus program, it is even more difficult to avoid the privacy violation. The State Commissioner for Data Protection and Freedom of Information notes that "especially when working with a service provider outside the direct influence of the person responsible, it's vital to guarantee a consistently reliable IT security."[2]

Many IT security managers struggle to detect data leaks in their own IT infrastructure. Cloud computing and the use of mobile devices and storage media have resulted in a large part of data being stored outside corporate networks. The result of using mobile devices in the Cloud is that breaches at service providers, suppliers, consultants, and other business partners now pose an even greater challenge than internal data leaks.

[1] Der Hessische Beauftragte für Datenschutz und Informationsfreiheit (2019, August). Datenpanne bei Mastercard und Mastercard Priceless. https://datenschutz.hessen.de/pressemitteilungen/datenpanne-bei-mastercard-und-mastercard-priceless

[2] IBID

A common source of data leaks are subsidiaries or partners (suppliers, law firms, architects, tax consultants, consulting firms) with a less stringent security architecture than that of their client. These enterprises often handle very sensitive documents, which can lead to industrial espionage, especially for internationally operating companies.

Third-party data leaks are challenging

Ponemon Institute studies show that cybersecurity is a growing challenge in the supply chain. Fifty-six percent of companies report that they have suffered a data breach caused by one of their supply chain partners.[3] The combination of increasing amounts of data stored, exchanged, and processed outside the company firewall, plus the lack of visibility into the cybersecurity measures along the entire supply chain, leaves many Chief Information Security Officers scrambling to address an increasing number of third-party data breaches.

Often companies are made aware of a data breach not by a third party, but by customers who report that they discovered personal data on the Internet. The security breach and lack of communication with customers can not only damage a company's reputation, but also diminish customer trust in a company.

Third-party data leaks can significantly increase the time it takes to fix the data leak, which puts data at risk longer than necessary. This delay increases the likelihood that reporting obligations may also be violated because the company did not take steps to report the possible data breach. Many companies are ill-prepared to deal with such third-party data leaks that require third-party contacts, contractual knowledge, and processes.

Digital transformation increases third-party risk

German industry is in the midst of the digital transformation propelled by Industry 4.0, which is heavily dependent on a secure supply chain. Third-party sabotage, data theft or espionage has cost the German economy a total annual loss of 102.9 billion Euros, according to a study by Germany's digital association Bitkom.[4] Three quarters of the companies were affected by attacks in the last two years, and another 13% suspect an attack. There is uncertainty as to whether data leaks have occurred or not; however, such uncertainty is risky and can lead to data breaches being detected, reported, and remediated too late.

Third-party sabotage, data theft or espionage has cost the German economy a total annual loss of

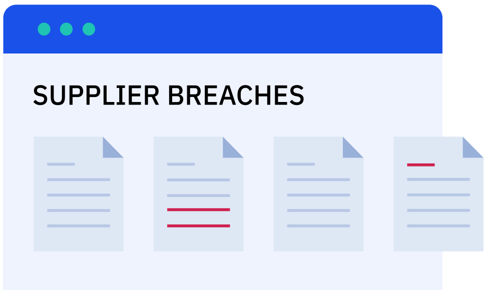
€ 102.9B

[3] Business Wire (2018, November). Opus & Ponemon Institute Announce Results of 2018 Third-Party Data Risk Study. https://www.businesswire.com/news/home/20181115005665/en/Opus-Ponemon-Institute-Announce-Results-2018-Third-Party

[4] Bitkom (2019, November). The damage is thus almost twice as high as two years ago. 2016/2017: 55 billion Euros p.a. https://www.bitkom.org/sites/default/files/2019-11/bitkom_wirtschaftsschutz_2019_0.pdf

CybelAngel detects data leaks across Supply Chains

Since 2013, CybelAngel, a global provider of digital risk management services, has been protecting well-known companies from data leaks, such as Sanofi, Danone, Air France and Total. “By combining our advanced AI-powered core detection technology with professional remediation services, we give enterprises an end-to-end cyber risk management solution that no other vendor can match,” says Erwan Keraudy, CEO, CybelAngel. “Because more data is being stored outside the firewall on cloud services, open databases, and connected devices, the risk to enterprises has never been greater. Our platform continually detects data leaks and incidents, which we then resolve with our remediation services, so businesses can eliminate exposure before damage occurs.”[5]



In order to minimize major digital risks such as compliance breaches and industrial espionage, CybelAngel enables clients to take proactive measures against data breaches. The CybelAngel portal acts as a threat intelligence headquarters where enterprises can see their exposure to data leaks, and interface with CybelAngel analysts. Companies gain insight into the security of their supply chain and are supported in complying with reporting requirements through in-depth reports on data leaks.

Using the CybelAngel portal eases pressure on Security teams. Instead of hunting down false positives, Security teams can concentrate on solving real issues. CybelAngel’s professional data leak remediation services ensure that risks are remediated nearly 85% faster than by other measures. CybelAngel provides an end-to-end solution to detect and fix undetected data leaks.

[5] Business Wire (2020, February). CybelAngel Introduces New Data Leak Detection Perimeters and Professional Remediation Services. https://www.businesswire.com/news/home/20200225005205/en/CybelAngel-Introduces-New-Data-Leak-Detection-Perimeters

About CybelAngel

CybelAngel reduces global enterprise digital risk by detecting critical data leaks outside the firewall before these leaks become major data breaches. Leveraging its Augmented Intelligence, a unique combination of proven machine learning capabilities and superior cyber analysts, CybelAngel analyzes billions of data sources, thousands of files, and hundreds of threats across all layers of the internet to discover critical data leaks for their customers. Global organizations rely on CybelAngel every day to detect critical data leaks before wreaking havoc on their business.

Learn more at www.cybelangel.com

PARIS, FRANCE | NEW YORK, NY