As Cyber Attacks Target Large Corporates, Teams Need to Evolve Data Security

By Karthikeyan Mariappan, VP of Engineering, Titaniam

Chief information security officers (CISOs) and their teams zealously study attack data to determine how adversaries' strategies are changing from month to month and year to year. Titaniam's recent research report, Enterprise Security Priorities for 2023, should put enterprise CISOs on notice. The reason why: in 2023, cybersecurity professionals predict that attackers will target large corporations over vertical-focused enterprises; insider threats will rise; and adversaries will seek structured and unstructured data that reveals corporate intent. The report surveyed cybersecurity experts at 100 enterprises to gain their predictions for 2023 and compared them to 2022 attack types and other breach findings.

Large Corporates Replace Financial Services as Most Targeted Sector

In 2022, respondents said financial services (36%) topped the data breach list due to its wealth of personal identifiable information (PII) and transaction data. This data can be held hostage via ransomware attacks, used to commit fraud, or leveraged to amass rich consumer profiles that can be sold on the criminal underground, to name just a few attack strategies.

In 2023, survey respondents expect 41% of attacks to target large corporations without a specific industry focus, up from 29% in 2022. So, what's the reason for attackers' newly industry-agnostic focus?

The fast pace of change has introduced new vulnerabilities into corporate networks. Large companies are adopting more cloud services, aggregating data for analytics, pushing code into production faster, and connecting applications and systems via APIs. As a result, misconfigured services, unprotected databases, little-tested applications, and unknown and unsecured APIs abound.

All of these changes make corporations attractive targets for cyber attackers, who often pivot to where the low-hanging fruit is. After all, why execute an automated distributed denial of service (DDoS) attack when you can simply look for and access an ill-secured cloud database or API?

Two-Thirds of Companies Reported Breaches, But Dwell Time Decreases

Given the rapid rate of change in 2022, it's not surprising that data breaches increased. Nearly two-thirds (65%) of companies reported data breaches in 2022, as attackers exploited process gaps and security vulnerabilities to exfiltrate data, 80% of which was not PII.

If there is a small silver lining to all of this bad news, it's this: Security teams are detecting breaches faster. Among those breached, 45% of security operations teams detected the incident on the same day, another 46% on the next day or up to a week, and a final 9% identified it within a month. Teams are using security platforms that leverage automation and artificial intelligence to detect anomalies amidst the noise and speed up security operations processes. This means less dwell time in networks for hackers and less damage for companies.

Malware, Insider Threats, and Ransomware Expected to Be Top 2023 Challenges

Malware threats will continue to be the top threat in 2023, representing 40% of expected threats. What's new for 2023 is that insider threats are the new number-two attack vector, predicted to represent 23% of attacks followed by ransomware and related extortion (21%) and phishing (16%). In 2022, the top threats were malware (30%), ransomware and extortion (27%), insider threats (26%), and phishing (17%). An important thing to note about these findings is that threats can be overlapping. For example, insiders can help launch ransomware attacks, while phishing attacks can also involve malware.

CISOs know that bad actors are using new malware types, such as loaders, info stealers, and wipers, to accelerate attacks, steal sensitive data, and create mayhem. They're also buying and stealing employee credentials to walk in through the front door of corporate networks. Attackers have realized that some companies don't use behavior-based analytics to detect abnormal activity from supposedly authorized users and are exploiting this gap to cause mayhem.

The Enterprise Data Types That Attackers Want Is Changing

Once inside networks, attackers move swiftly to locate and exfiltrate desired data. Surprisingly, PII is no longer the top target. Instead, in 2022, hackers exfiltrated high-value data, such as data crucial to the organization (57%) and intellectual property (57%) over PII or sensitive PII (38%). (Some data represents more than one type of information.)

Survey respondents predict that in 2023 attackers will target structured data used for analytics (68%) over that used in databases (62%). They'll also target unstructured data created by users (58%) over that created by applications (54%) or other sources (16%). This is a reversal from 2022 when attackers targeted structured data used in databases (68%) over analytics data (63%) and unstructured application data (57%) over user data (50%).

The reason for this change of heart? Analytics and user data reveal corporate intent, providing a lens into strategies, product launches, sales targets, partnerships, and other plans of interest to attackers, such as nation-states, cybercriminals, and more. Meanwhile, malicious insiders can easily sell this data externally to a myriad of buyers.

Why Protecting Data Is the New #1 Security Priority for Corporate Teams

Large-scale data breaches are always harmful to companies. However, losing control over go-to-market strategies, intellectual property, and other sensitive data can quite literally derail a company's future. Nation-states can use stolen intellectual property to take solutions to market faster and corner a niche. Competitors can poach customers by offering better deals. Analysts can downgrade companies' ratings based on leaked plans. The list goes on and on.

So, it's not surprising that protecting data (31%) has emerged as the #1 security priority for 2023, ahead of preventing ransomware, data exfiltration, and extortion (27%); and staying ahead of malicious attacks (23%) and other objectives. To achieve this goal, 92% of teams plan to increase their security measures in 2023, while 97% will explore new solutions.

How Corporate Cybersecurity Teams Will Protect Data in 2023

Cybersecurity teams plan to use a variety of techniques to protect data from unauthorized access and exfiltration. Increasingly, they're choosing modern or next gen tokenization (60%) over traditional tokenization (49%), both of which swap sensitive data for tokens. That's because modern or next gen tokenization systems implement encryption-in-use on the back end enabling teams to be able to search and analyze information without detokenizing it. With traditional tokenization, teams are forced to ust detokenize data to use it, and this leaves the data exposed to attacks.

Similarly, cybersecurity teams want to leverage data masking (58%), ensuring private data is not visible to unauthorized users. They're also relying on encryption-in-use (55%) to bolster data protections, not just encryption-at-rest (51%) and encryption-in-transit (51%). Encryption-in-use keeps data secure while apps and databases query and analyze it. Companies that don’t have that capability risk exposing data whenever it’s used, which is often.

While rising data risks and beaches are obviously a concern for cybersecurity teams, the good news is that they can use multiple techniques to minimize these threats. Platforms that use modern or next gen tokenization, data masking, and encryption across the data lifecycle can protect organizations against exfiltration and ransomware demands while still making information available for search and analytics.

About the Author

Karthikeyan is the Co-Founder and Head of Software Development at Titaniam. Before Titaniam, Karthikeyan spent 15 years at Yahoo where he spearheaded data analytics solutions. Karthikeyan believes that not only remote workplace was a necessity during the pandemic, it will be a significant part moving forward and keeping employees engaged requires a different approach.

Karthikeyan can be reached online LinkedIn and at our company website https://titaniam.io/.