Analyzing API-Related Breaches: Insights from SEC Disclosures

Introduction: The Rising Risk of API Security Failures in Public Companies

As businesses accelerate digital transformation, APIs have become the backbone of modern applications, facilitating seamless connectivity and data exchange. However, this increased reliance on APIs has also introduced a growing attack surface that cybercriminals are actively exploiting. A review of recent SEC filings reveals a troubling trend: API breaches are not only frequent but are also leading to regulatory scrutiny, financial losses, and reputational damage.

High-profile companies across industries—including telecommunications, financial services, and technology—have disclosed API-related security incidents that have exposed sensitive customer data, authentication credentials, and business-critical systems. These incidents have led to regulatory investigations, SEC settlements, and, in some cases, lawsuits alleging failure to disclose cybersecurity risks. This brief highlights key API-related security breaches reported in SEC filings and underscores the urgent need for enterprises to strengthen their API security posture.

Confirmed API-Related Breaches in SEC Filings:

1. **T-Mobile US, Inc. (2023)** – API exploited to access customer account data.
2. **Dropbox, Inc. (2024)** – Threat actor accessed API keys, OAuth tokens, and authentication data.
3. **SolarWinds Corporation (2020)** – API vulnerabilities were exploited as part of the supply chain attack.
4. **Robinhood Markets, Inc. (2021)** – API-related breach led to exposure of millions of customer records.

5. **Mimecast Limited (2020)** – Attackers accessed API authentication keys in the SolarWinds attack.
6. **Avaya Holdings Corp. (2020)** – API vulnerabilities linked to SolarWinds-related breaches.
7. **Check Point Software Technologies Ltd. (2020)** – API security weaknesses contributed to breach.
8. **Unisys Corporation (2020)** – API misconfigurations were part of its SolarWinds-related breach.
9. **Ashford Inc. (2023)** – API exploitation suspected in a breach affecting 46,000 individuals.
10. **SolarWinds Corporation (2024)** – API security failures were part of an SEC lawsuit regarding disclosure practices.

Conclusion: API Security is Now a Boardroom Issue

The SEC's increasing focus on cybersecurity disclosures makes it clear: API security is no longer just a technical concern—it's a boardroom imperative. As API-driven attacks continue to make headlines, companies that fail to implement robust API security measures risk regulatory penalties, legal consequences, and severe reputational harm.

To mitigate these risks, organizations must prioritize continuous API discovery, proactive threat detection, and automated runtime protection. Modern security strategies should move beyond traditional perimeter-based defenses and adopt an attacker's perspective to identify and remediate vulnerabilities before they are exploited.

The recent wave of SEC filings serves as a wake-up call: API security is no longer optional. Companies that fail to address these risks now may find themselves in the next headline—or worse, in front of regulators.

These filings demonstrate a growing trend where API security flaws have been central to major data breaches. If you need more details or want to dig into specific SEC documents, get in touch with us today!