Third Party Vendor Risks and What you Should Know

Introduction

In 2022, a spike in targeting third-party vendors almost doubled from 2021, with 63 attacks on vendors being reported and 298 victims. This trend of increasing attacks on third-party vendors has only continued in Q1 of 2023 as several third-party vendors have reported being attacked by malicious campaigns. There are several dangers when third-party vendors are attacked. The insight the primary organization has into their vendors' security protocols is reported as extremely limited as only 11% of companies feel they understand each party's cyber security and practices. Only 32% of organizations report that they believe their suppliers will let them know in the instance of a breach. It was found that the average disclosure time between a breach occurring, and the vendor being notified was 108 days (about 3 and a half months). This was an increase of 50% from 2021 which provides threat actors with an additional month of time increasing the potential damage against vendors with stolen data.

Root Causes

There were four common root causes in 2022 that lead to third-party breaches.

1. Unauthorized network access accounted for 40% of third-party breaches in 2022 and was the most-common attack vector. These types of attacks generally originate from social engineering attacks through targeted phishing campaigns. Threat actors try to gain access to the network through stolen credentials or exploiting known vulnerabilities or a combination of the two.

2. Ransomware accounted for 27% of third-party breaches, coming in second as the most frequent root cause in 2022. These attacks rely on threat actors acquiring internet infrastructure and maintaining ways to process payments which has become more difficult as monitoring of crypto currency has increased.

3. Unsecured servers and databases made up 10% of third-party breaches ranking third in 2022. Unsecured assets, such as databases and servers, present a significant risk to companies allowing threat actors easy entry. If a third-party manages PII (Personal Identifiable Information) on behalf of another organization, this risk can be even greater.

4. Misconfigured server-caused incidents, such as third-party breaches, were also noted as a potential risk in 2022. This type of issue has become associated with cloud vendors or advertising companies leaking sensitive data. However, when an organization uses a cloud service, there is a shared responsibility for maintaining the security of any information stored in the cloud. Server misconfiguration attacks exploit configuration weaknesses or security vulnerabilities found in web servers and application servers. Often cloud companies or advertising companies assume that the responsibility of security is with the primary organization, while the organization assumes that the third-party vendor is responsible for the security.

Industries Impacted

The most frequently impacted industries in 2022 were healthcare, finance, and government. The healthcare industry represented 34.9% of breaches within 2022. Threat actors view the healthcare sector as a prime target due to an abundance of personal information that lacks the budget for secure communication methods and updated software.

The finance sector was the second sector most impacted by third-party attacks. This sector is known by threat actors to be one of the most vulnerable industries, due to banks working with several vendors for faster transactions and applications. To improve their processes, financial institutions typically grant access to sensitive data, vital systems, and other critical resources to their third-party vendors.

Government organizations were the third most targeted, as government agencies have multiple vendors creating a cast digital supply chain. The data these third-party vendors have access to is considered valuable and diverse, often pertaining to critical infrastructure. This makes the sector a prime target for threat actors.

Additionally, in 2022, technology vendors were assessed to be the most at risk for third-party breaches. Threat actors were targeting technology vendors through vulnerabilities in software to edit code for exploitation. These types of exploitations in the supply chain can lead to some of the most damaging to organizations. These vendors were targeted in 30% of incidents.

Conclusion

Organizations that enter relationships with third or fourth-party vendors put clients at greater risk of data breaches and other forms of cyberattack. Research has found that the more third parties an organization depends on, the higher the frequency of breaches and data leaks the organization is susceptible to. Organizations and their Managed Security Service Provider (MSSPs) need to understand the risks associated with managing third parties and to take steps toward lessening the risks.

The Critical Start Cyber Threat Intelligence (CTI) team will continue to monitor the situation and work closely with the Threat Detection Engineering (TDE) team and the SOC to implement any relevant detections. For future updates, the CTI team will post via ZTAP® Bulletins and on the Critical Start Intelligence Hub.

References:

1. https://blog.cyble.com/2023/02/10/u-s-telecommunications-companies-targeted-consumers-hit-hardest/
2. https://www.msspalert.com/cybersecurity-news/third-party-risks-challenges-for-mssps-and-how-to-overcome-them/
3. https://www.helpnetsecurity.com/2023/02/27/third-party-risks-erm/
4. https://www.csoonline.com/article/3688909/cyberattacks-hit-data-centers-to-steal-information-from-global-companies.html#tk.rss_all
5. https://blackkite.com/wp-content/uploads/2023/01/third-party-breach-report-2023.pdf
6. https://www.darkreading.com/attacks-breaches/controlling-third-party-data-risk-should-be-a-top-cybersecurity-priority-