Isaac Piegat
Professor Howard-Stone
October 23rd, 2024
Business Security

In today's modern world, data privacy is more important than ever. Since businesses rely more on technology and cloud services everyday, they become ever better targets for hackers and other threats. Hackers themselves are getting more sophisticated, finding new and unique ways to access sensitive information, putting entire companies and their clients at risk. This essay plans to explore emerging threats in data privacy, the battle for security, and ways businesses can boost their own security.

An immediate threat in need of attention are "social engineering attacks". Among these types of attacks include phishing and spear-phishing like sending fake emails to employees hoping they'd reveal some information or worse, grant unauthorized access. As the internet gets older, these attacks have become more sophisticated and refined, allowing hackers to frequently impersonate executives or key business personnel to manipulate employees more effectively. To combat this, employees need to undergo tra...

Another major concern is ransomware attacks using "double-extortion" tactics, allowing them to not only encrypt data but also threaten to publicize it unless a sum is paid. Not only would a company lose critical data, but the company would face reputational damage if the data is sensitive. To further make things worse, attackers are targeting supply chains, infiltrating third-party vendors indirectly gaining access to company systems. Combatting this would require a new approach to security, including v...

Zero-day exploits are also on the rise. These attacks target previously unknown software vulnerabilities, giving hackers a window of opportunity to breach defenses before patches are released. The unpredictable nature of these exploits means that companies must stay proactive with frequent vulnerability scanning, regular updates, and continuous monitoring to quickly address potential risks.

To effectively address these threats, businesses need to treat security with utmost importance. Implementing multi-factor authentication is a simple yet powerful step. It should be mandatory for all important applications, and adaptive authentication techniques can further enhance protection by analyzing user behavior and device risks. Beyond authentication, data encryption and tokenization are useful. Encrypting data both at rest and in transit means that even if data is stolen, it's useless without t...

Regular penetration testing and "red team" exercises are crucial in identifying vulnerabilities. These tests simulate real-world attacks, giving companies useful insights into their defenses and areas for improvement. Red team exercises, where experts actively attempt to breach systems, can be particularly effective in funding hidden weak points. Automating "incident response" is another key measure. Automated systems can detect and isolate breaches quickly, preventing compromised accounts or devices fro...

A longer-term strategy for boosting data privacy is adopting a Zero Trust Architecture (ZTA). The Zero Trust model operates on the principle of "never

trust, always verify," requiring ongoing authentication for every device and user accessing company resources. This approach significantly reduces risks by eliminating implicit trust within internal networks and limiting an attacker's ability to move laterally if they break through the outer defenses.

It's also important for companies to prioritize privacy by design, embedding privacy-enhancing technologies like encryption and differential privacy from the beginning of the development process. This proactive approach ensures that privacy is considered from the outset, rather than being an afterthought.

Building a Zero Trust Architecture by focusing on privacy by design and training employees are key steps to ensure long-term data privacy. By taking these steps, businesses can protect sensitive information and maintain the trust of their clients and stakeholders in a changing digital landscape.

Bibliography

- TechRadar. "Ransomware, AI, and Social Engineering All Set to Be 2024's Biggest Security Threats." TechRadar, 7 Nov. 2023, www.techradar.com. Accessed 23 Oct. 2024.
- Palo Alto Networks. "The Evolving Threat of Ransomware — A Call to Action for Cybersecurity." Palo Alto Networks, www.paloaltonetworks.com. Accessed 23 Oct. 2024.
- PwC. "Zero Trust Architecture: A Paradigm Shift in Cybersecurity and Privacy." PwC, www.pwc.ch. Accessed 23 Oct. 2024.