Hi Michael,

Thank you for sharing your post on Microsoft Azure’s vulnerabilities. I’ll say that it’s pretty interesting to see that even a high-profile cloud service, such as Azure, can be vulnerable to some serious exploits like request spoofing and even remote code execution. We tend to think that organizations, like Microsoft, have the capital and workforce to ensure they push out secure code and this is a reminder that even the most well-funded organizations are still susceptible to hackers.

When comparing this story of Azure’s CVE discovery with the IoT vulnerabilities I read about, there are some interesting differences in the types of exploits each industry faces. Within the tech industry, especially with cloud services like Microsoft Azure, there’s a lot at stake in terms of data privacy and control. The truth is that a breach within cloud services doesn’t just yield an impact for one device or individual—it could give attackers access to entire virtual machines or even complete control over applications running on the platform; which is massive for businesses relying on these services (Kumar, 2020). The request spoofing flaw (CVE-2019-1234) allowed unauthorized access to sensitive data through Azure Stack’s API and the remote code execution flaw (CVE-2019-1372) enabled attackers to potentially control entire Azure servers. This would be not only devastating for the Microsoft corporation but all who utilize this platform for their cloud computing business needs.

Within the realm of these types of exploits, organizations within the tech industry will find this critical to their business model because they’re overseeing vast amounts of data from a range of clients and other sectors. A good example, as referenced by Kumar (2019) from the impact of CVE-2019-1234, would be an attack targeting Azure impacting any organization that is using Azure Stack for their hybrid cloud solutions such that it could disrupt business processes on a large scale. Compared to the IoT space, where security issues often come from the lack of authentication measures or even hardcoded passwords (Spektor, 2024), cloud services require substantial cybersecurity practices such as proactive investment in API security that once resulted in “a way to get the virtual machine name and ID, hardware information like cores, total memory of targeted machines, and then used it with another unauthenticated HTTP request to grab screenshots” (Kumar, 2020).

The relevance of these threats for a company like Microsoft and its competition is massive since these industries are often providing the infrastructure needed for many clients and other important industries. Such compromises would not only risks Microsoft’s reputation but also impact their clients’ operations. It really shows why cloud providers need to maintain rigorous security practices, including patching and secure API management, to stay ahead of these types of threats.

Cheers,

Sean

References:

Kumar, M. (2020, January 30). *Microsoft Azure Flaws Could Have Let Hackers Take Over Cloud Servers*. The Hacker News. https://thehackernews.com/2020/01/microsoft-azure-vulnerabilities.html

Spektor, H. (2024, July 28). *Top 10 IoT vulnerabilities and how to mitigate them*. Sternum IoT. https://sternumiot.com/iot-blog/top-10-iot-vulnerabilities-and-how-to-mitigate-them/

Hi Putt,

I appreciate your post regarding power grid vulnerabilities highlighted by the GAO report, and I had no idea that we had students from East Asia—so, welcome! As someone who is directly involved in aspects of the United States’ critical infrastructure management, it’s definitely concerning to see how important infrastructure like the power grid could be at risk, especially from something as prevalent as IoT devices. This, along with other noted aspects regarding the potential vulnerabilities to industries like energy, where a successful attack could disrupt not just one company but entire regions relying on power, highlights just how vulnerable our nation’s critical infrastructure could be to persistent threat actors.

Energy infrastructure security is indeed unique, and I would venture to guess that your average citizen doesn’t think much about the potential threat vectors associated with it. Unlike the data-focused concerns seen in many tech sectors, power grid vulnerabilities directly affect physical services, making an attack here a different type of risk altogether. In such industries as the marine transportation system, access to the power grid is paramount for ensuring continuous supply movement for the nation and any disruption associated with it would not only cripple the nation’s economy but impact the average citizen due to lack of necessary goods. In reference, the GAO report shows that with IoT devices embedded in power facilities, there are not only digital but also physical access points that can be exploited (Venkat, 2019). A good example as stated by Venkat (2019) is in the March 2019 DDoS attempt, malicious actors targeted the power utility’s network, and while there was no disruption of power, hackers identified gaps within the communications between two stations. This impact is an important reminder of how Advance Persistent Threats (APT) could consistently enumerate aspects of our critical infrastructure that could lead to wreaking havoc on the entire country.

In contrast with my subject on consumer IoT, typical attacks often stem from unprotected devices with weak authentication or outdated firmware, which can be leveraged for botnet attacks (Bodnar, 2024). But in the energy sector, the consequences of a breach go beyond individual devices and according to Venkat (2019), the potential usage of botnets through the compromising of different IoT devices could be used to turn against a powerplant or utility. Additionally, malware attacks, like the one in Ukraine in 2015, revealed how a targeted approach could disable key systems and result in massive power outages. In fact, reading these types of potential threat vectors reminds me of the Stuxnet worm, which was originally deployed to sabotage Iran’s nuclear centrifuges in 2010. This type of exploit demonstrated how malware could be engineered to target some industrial control systems (Britannica, 2024), which are commonly found within sectors like energy and utilities; a glaring reminder of what might happen to our own power grid. As such, securing this important infrastructure requires strong, complex defenses that would be able to address both the networked devices and the operational technology in power plants.

For organizations in the energy sector, these insights highlight the importance of monitoring not just the digital network but also physical access to systems to maintain secure, uninterrupted power supply.

Cheers,

Sean

References:

Bodnar, D. (2024, July 23). *10 IoT vulnerabilities to be aware of + protection tips*. Norton. https://us.norton.com/blog/iot/iot-vulnerabilities

Britannica, T. Editors of Encyclopaedia (2024, September 23). *Stuxnet*. *Encyclopedia Britannica*. https://www.britannica.com/technology/Stuxnet

Venkat, A. (2019, September 27). *GAO raises concerns about power grid vulnerabilities*. https://www.bankinfosecurity.com/gao-raises-concerns-about-power-grid-cybersecurity-a-13157