RAPID7

2021 Vulnerability Intelligence Report - Boardroom Takeaways

For many security professionals, 2021 was one of the most difficult years on record. Many high-profile issues made it into the public consciousness in ways they hadn't in the past. Based on the findings of our annual Vulnerability Intelligence Report, this document offers much needed context to help you understand what these findings mean for your business moving forward.

Worsening Security Landscape

- The threat of cyber-attacks has increased significantly over the past year for the average corporation. Those tasked with defending the organizations have had a particularly tough year, dealing with new vulnerabilities that pose serious threats. Availability of defensive security talent has also been significantly outstripped by the volume and speed with which attackers can now act.

- In 2021, we are seeing many more new vulnerabilities emerge that are easier to exploit, enabling potentially less sophisticated attackers to be able to weaponize them to target average businesses. We are also seeing a larger volume of attacks in general. This means the average businesses and organizations are increasingly in the cross-hairs of cyber criminals.

The Vulnerability Paradox

- In years past, the more sensational vulnerabilities or hacking incidents did not necessarily correlate to widespread attacks, despite the publicity. This is partly due to the fact that these vulnerabilities were challenging to exploit and required a level of sophistication few attackers possessed. Therefore, only well-resourced attackers such as nation-states were able to leverage them, and the target of such attacks tended to be strategic assets, or organizations representing significant financial value to the attackers. Lack of wide-spread attacks means the probability of an "average business" being targeted was relatively low.

- In recent years, it is frequently those vulnerabilities in ubiquitous technologies that posed the most threat. These vulnerabilities can be pervasive as they reside in popular software and appliances many businesses use. Their near omnipresence means they are no longer reserved for nation-state hackers or otherwise well-resourced attackers. They are also no longer leveraged solely for "high-value" targets. These vulnerabilities allow for more widespread attacks, which means average businesses are more likely to be a target. Yet, perversely, boardrooms and C-suite are likely to pay less attention to them as the resulting attacks tend not to be as newsworthy. (Examples include critical SAP and Microsoft vulnerabilities like the ones noted in the main report).

"7 Days to Boom"

- Not only do we see more of these new vulnerabilities surface that allow for widespread attack on average organizations, we are also seeing a shortened window between when the vulnerabilities are discovered and when they become leveraged in widespread attacks.
- This means a significantly shortened window for security teams to patch the vulnerability in order to prevent attacks. This considerably strains the already stretched security resources of many organizations.
- Having a well-developed emergency patching procedure as well as a generally robust incident response procedure would be very beneficial. But in order to have robust emergency procedures, security teams need to build a strong foundation of proactive asset and vulnerability management programs. It is not realistic to expect a security team that is still struggling with resourcing for foundational security program activities to have strong emergency procedures.

Advice to the C-Suite and Boardroom

- C-Suite and Boardroom need to recognize the increasingly widespread nature of security threats and the very real prospect that attack targets are increasingly the average businesses rather than "strategic" or "marquee" businesses only. What's more, boardrooms need to start funding for more security resources and emphasize basic security hygiene which will allow InfoSec teams to build a strong foundation rather than the reactive mode many are currently in, which often falls short of being effective and are not sustainable over time.

For the full Rapid7 Vulnerability Intelligence Report click here