Trend Research

The Increasing Strategic Risks of Natively Connected IoT Devices and How to Manage Them

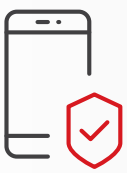
This primer outlines the increasing risks presented by Internet of Things (IoT) devices that operate beyond the bounds of traditional cybersecurity measures. Understanding these developments is critical because these situations create opportunities for attackers to take advantage of visibility gaps and side channels that most organizations cannot monitor and that contribute to the expansion of their attack surface. We explain how the risks associated with these devices are becoming more intense and what strategies to adapt to secure your networks and data.

Key Takeaways

IoT risks are not new, but the level of maturity among cybercriminals today is leading to an ongoing paradigm shift. This is exemplified in the way cybercriminals and state-sponsored groups are exploiting the security limitations and increased connectivity of IoT devices. Attackers have been found using operational relay box (ORB) networks and eternal botnets, which has had a similar impact to the change in tactics, techniques, and procedures (TTPs) from the transition to living-off-the-land (LOTL) attacks in recent years.

Chief Information Security Officers (CISOs) need to factor in these challenges for their risk modeling, security measures, and vulnerability patching, requiring organizations to reassess or update their security models to address evolving security threats. The growing number of IoT devices makes organizations more susceptible to potential attacks. CISOs must lead efforts in updating security measures and ensuring that risk models address these evolving threats.

Various technologies allow unexpected connectivity and side channels for attackers, presenting security challenges for indoor and outdoor IoT devices. The increase of IoT devices in both indoor and outdoor environments resulted in the development of different technologies, leading to unexpected connectivity and side channels in areas where there should be none. This situation further raised the difficulty of securing these devices.



The increasing use of IoT devices raises concerns about privacy, threats to critical infrastructure, and cybersecurity risks for businesses, governments, and individuals. In the face of these challenges, it's crucial to implement comprehensive security measures and strategic risk management. This highlights the importance of thorough security measures in the current landscape of IoT connectivity.

Trend Research

TREND MICRO

Mitigating Risks Associated With Increased IoT Connectivity

It's critical to mitigate the risks associated with the growth of natively connected IoT devices given the security blind spots that it can introduce within organizations. To adapt, organizations must take immediate action by carefully reassessing their security models and measures. To learn more about how organizations can minimize such risks, read this article: https://research.trendmicro.com/unwired.