Strengthening Japan's Cybersecurity:

DeviceTotal For Emerging Threats Mitigations

Japan's Cybersecurity Challenges

Japan faces a growing wave of cyber threats, particularly from state-sponsored actors, with critical infrastructure being a primary target. Kazutaka Nakamizo, deputy director of Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC), highlighted these issues at the Munich Cyber Security Conference. He noted that cyber incidents surged from 150 in 2021 to 230 in 2022, and the trend continued upwards last year, representing "just the tip of the iceberg."[1]

Organizations in Japan faced an average of 1,003 cyberattacks per week, with FakeUpdates being the most prevalent malware. Most malicious files were delivered via email, and Remote Code Execution was the most commonly exploited vulnerability.

The average cost of a cyberattack in Japan is USD 4.52 million.

Nakamizo emphasized that many attacks remain unattributed publicly, with several exploiting unknown vulnerabilities in networks. He stated, "Japan sees increased cyberthreats to critical infrastructure, particularly from China."

[1] https://therecord.media/japan-critical-infrastructure-cyberthreats

Most impacted industries in Japan in the last 6 months:

Industry	No. of attacks
Manufacturing	908
Software vendors	738
finance/banking	572
Retail	508
ISP/MSP	384

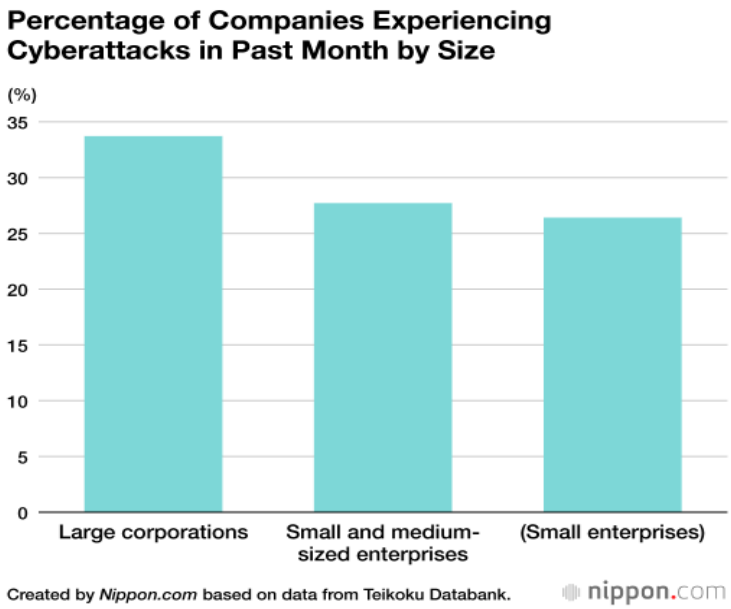
Japan's response to these threats involves strengthening international cooperation, particularly with the United States. In September, Japanese and U.S. agencies issued a joint advisory on China-linked cyber actors.

Recent cyber incidents in Japan included breaches in the Ministry of Foreign Affairs, the aerospace exploration agency JAXA, and several major corporations like Yamaha, Seiko, Casio, and Eisai. These attacks underscore the urgency for robust cybersecurity measures.

The number of cyberattacks in Japan is surging as hackers try to exploit the country's weak defenses. Japan has lagged other advanced nations in updating systems to detect attacks and protect data, according to cybersecurity experts[2].

Japanese businesses, in particular, rely heavily on outside vendors for systems development and have been slow to fix software once vulnerabilities are discovered.

[2] https://asia.nikkei.com/Spotlight/Datawatch/Cyberattacks-on-Japan-soar-as-hackers-target-vulnerabilities



As a recent report[3] by FORESCOUT demonstrates, risks from exposed devices are dramatically high:

- There are nearly 17 million internet-accessible devices in Japan. See the breakdown by cities in the below image.
  75% of these devices are routers, networking equipment, and security appliances, including VPNs. Additional devices at risk are IP cameras and building automation systems.
- Many OT devices use vulnerable protocols like Modbus, BACnet, Fox, and KNX, making them targets for attackers.

[3] https://www.forescout.com/blog/cyber-threat-landscape-in-japan-risks-threats-mitigation-guidance/

- Devices with exposed firmware versions are at risk of being exploited based on known vulnerabilities.

  These devices can be directly attacked by opportunistic or targeted attackers who can interact with protocols that require no authentication. In some cases, they can directly access human-machine interfaces (HMIs) that provide start/stop or configuration capabilities.

DeviceTotal's Role in Addressing Those Challenges

DeviceTotal, a comprehensive cybersecurity platform, is designed to address those challenges in an innovative and risk-free way. Powered by ML technology, DeviceTotal leads in exposure management, helping organizations and governments stay ahead of emerging threats, providing proactive defense for every connected asset, from OT, to IoT and network devices. DeviceTotal excels in providing up-to-date and precise security information, sourced directly from vendor's advisories, allowing timely and proactive threat elimination. Here is how:

- Real-Time Vulnerability Management and Threat Intelligence:
    - Proactive Monitoring: DeviceTotal continuously monitors the vendor's advisories, identifying vulnerabilities and potential threats in real-time. This capability helps mitigate risks also associated with vulnerabilities exploited by state-sponsored actors .
    - Actionable Insights: The platform provides actionable insights to address vulnerabilities before they can be exploited, aligning with Nakamizo's emphasis on tackling the root causes of cyber threats .
- Enhanced Security Posture:
    - Comprehensive Visibility: DeviceTotal offers a clear overview of the security posture across all connected devices, helping organizations understand and strengthen their defenses against sophisticated threats .
    - Risk Assessment: By evaluating the risk level of each device, organizations can prioritize security measures and allocate resources effectively to safeguard critical infrastructure .
- Facilitation of Public-Private Partnerships:
    - Information Sharing: DeviceTotal supports enhanced information sharing between government bodies and private enterprises, fostering collaboration and unified response strategies. This feature aligns with
    - Japan's strategy to boost private-public partnerships for improved cybersecurity readiness .
- Compliance and Regulatory Support:

- Meeting Standards: DeviceTotal aids organizations in meeting regulatory requirements and maintaining compliance with
- Cybersecurity standards, which are vital for protecting sensitive data and maintaining trust.

By integrating DeviceTotal into its cybersecurity framework, Japan can enhance its ability to prevent, detect, and respond quickly to cyber threats. The platform's comprehensive capabilities support Japan's objectives of bolstering cybersecurity defenses and fostering international cooperation to combat sophisticated cyber adversaries.

Thank you,

Contact@DeviceTotal.com today!