BLUVECTOR®
A COMCAST COMPANY

How the Internet of Things Increases the Risk of a Cyberattack

The Internet of Things (IoT) is growing rapidly, both in consumer and business markets. In fact, 90% of companies claim that IoT adoption is critical to their digital transformation plans.

With the benefits of IoT come a higher level of security risk. These devices may have significant security vulnerabilities, expanding the corporate digital attack surface and contributing to cybersecurity risk. Making the most of an investment in IoT solutions requires ensuring that organizations properly monitor and secure these devices against potential cyber threats with network detection and visibility.

IoT Challenges

As IoT grows, the cyber data crunch increases, putting additional demands on cyber analysts. These day-to-day challenges may affect the speed and efficacy of your cyber workforce if you don't have automated processes and tools in place to help ease the lift.

Many IoT devices lack the resources required to process the data that they collect, and extract insights needed for necessary changes. Often, these resource-constrained devices are supported by cloud-based servers that aggregate and analyze the data collected by various IoT devices.

Security Risks Introduced by IoT

While IoT devices provide a number of benefits by collecting in-depth data from various sources and automatically analyzing and acting upon this data, they also introduce security risks.

The devices may have access to sensitive data, are connected to the Internet, and may contain security vulnerabilities that leave them open to attack – making organizations vulnerable.

Expanded Attack Surface

IoT devices are typically resource-constrained devices that collect large volumes of data for processing elsewhere. They rely upon cloud-based servers to process the data, extract conclusions, and send instructions in response.

By design, IoT devices are reachable from the public Internet to achieve connectivity with their cloud-based servers. If access to these devices is not strictly controlled via firewalls and access control lists (ACLs), they provide attackers with a potential entry point into the enterprise network. With a foothold on an IoT device, cyber threat actors can move laterally through the network to access other systems behind the network's perimeter-based defenses.

Poor Device Security

While leading IoT providers have made significant strides building security protocols, there remains a great deal of variance in IoT security among varying manufacturers. Some of the common IoT security issues that create a risk to an organization include:

- **Weak, Default, and Hardcoded Passwords:** IoT devices may come with hardcoded or default

passwords that many users do not or cannot change. This enables malware to log into these devices using these weak credentials and add them to botnets for use in Distributed Denial of Service (DDoS), credential stuffing, and other automated attacks.

- **Use of Insecure Network Protocols:** Unencrypted, insecure protocols like Telnet have been deprecated due to their exposure of login credentials and other sensitive data. However, IoT devices may use Telnet, enabling attackers to eavesdrop on their traffic and remotely access and control IoT devices.
- **Poor Use of Cryptography:** Encryption is essential to the security of both at rest and in transit. However, IoT devices may store data without the proper encryption or use insecure and incorrect implementations of cryptographic functionality that place data at risk.
- **Vulnerable Software and Third-Party Code:** IoT devices may have less secure development practices than other applications. As a result, their software is more likely to contain vulnerable code and to use outdated versions of third-party libraries that have known and actively exploited vulnerabilities.
- **Poor Update Management:** Frequent updates are essential to software vulnerability management. However, some IoT device manufacturers are slow to release timely updates after vulnerabilities are discovered, and few device owners think to check for and apply updates for IoT devices, such as smart lightbulbs or coffeemakers.

Sensitive Data Exposure

IoT devices are designed to collect and analyze data using a variety of different sensors. Depending on the use case, this may provide them with access to sensitive information. IoT devices may have access to sensitive information in an organization's operations, including intellectual property and trade secrets.

Poor IoT device security can place this data at risk. If an attacker can gain access to an IoT device or eavesdrop on its communications, then they could gain access to this data. Also, the use of insecure network protocols such as Telnet creates the potential for an attacker to modify data in transit, enabling them to modify commands sent to the IoT devices or the data collected by them that is used to make crucial business decisions.

Cyber-Physical Effects

IoT devices are designed to interact with the physical world. This includes both collecting information using various sensors as well as causing physical effects, such as Internet-connecting manufacturing equipment or a pacemaker. Poor IoT security means that these devices may be compromised by an attacker who could misuse this cyber-physical functionality. For example, an attacker could change manufacturing processes to perform a Denial of Service (DoS) attack, create defective parts, or introduce malicious functionality into manufactured components.

Solving IoT Security Challenges

Again, while leading IoT developers have made significant strides in cybersecurity, there remains a great deal of variance among IoT security protocols, and it can be difficult for organizations to know how secure their IoT devices – especially legacy devices – really are. Due to the resource constraints on many of these devices and the diversity of architectures, deploying on-device security solutions to each IoT device is infeasible for many organizations.

Protecting these devices against attack requires advanced cybersecurity solutions that operate at the network level. Critical capabilities include in-depth network visibility, advanced threat detection, and integrated threat hunting capabilities.

Network Visibility

Many organizations lack comprehensive visibility into their networks, leaving them blind to the devices connected to their network and how they are communicating. This is especially dangerous with the rise of the IoT. Employees may connect unauthorized devices to the network providing attackers with access points to the network, or attackers may target insecure IoT devices in their attack.

Comprehensive network visibility is an essential component of a corporate IoT security strategy.

Organizations need visibility into every device that is connected to their network infrastructure and insight into their communications to identify the use of insecure protocols, potential data exposure, and attempts by attackers to gain and exploit access to corporate IoT devices.

Threat Detection

As companies increasingly deploy IoT devices, cyber threat actors are targeting these devices in their attacks. IoT devices may contain unknown, unpatched vulnerabilities and use custom communications protocols that attackers might exploit.

Protecting these devices against attack requires the ability to detect threats and notify security personnel in near real time. Threat detection solutions can expedite the incident response process, enabling security personnel to take action to quarantine and remediate potential infections before they can access the network.

Threat Hunting

Cyberattacks are growing increasingly subtle and sophisticated, and some threats may slip through the cracks of an organization's defenses. These undetected attacks could allow an attacker to collect sensitive data or expand their access to the corporate network.

Threat hunting enables a company to find the attacks that evade its perimeter-based defenses. With access to in-depth security data and analytics, security personnel can identify and respond to these previously undetected attacks.

Security and Automation are Critical to IoT Success

IoT devices provide significant benefits to an organization, but also can create major security risks and put pressure on your cyber workforce if you do not have the proper processes and tools in place.

To gain the full benefit of its IoT deployment, an organization must first secure those devices to minimize the risk to its systems, data, and operations. BluVector's network protection and visibility, AI/ML threat detection, and threat hunting capabilities are essential to monitoring and securing a diverse collection of Internet-connected devices, while augmenting your current cyber security framework and increasing the efficiency of your cyber team. Learn more about how to improve your network visibility, security, and speed up your daily cyber operations by contacting BluVector for a demo.

ABOUT BLUVECTOR

BluVector is a machine learning innovator with more than a decade of experience applying AI to detect and hunt down cyber threats. BluVector solutions strengthen the cyber defenses and protect the assets of some of the world's most discerning customers. With multiple patents, BluVector continues to help customers leverage AI-based and automation approaches to manage the volume, velocity, and polymorphic nature of today's and tomorrow's cybersecurity threats.

BluVector
4501 North Fairfax Drive, Arlington, VA 22203
www.bluvector.io