ETHERIOS
A Division of Digi International

Securing the Internet of Things

How to Safeguard Your Devices in the New World of Connectivity

As a pioneer in the Internet of Things (IoT), Etherios grasps the promise and challenges of this new era of connectivity.

By 2020, according to the Gartner Group, over 26 billion IoT devices will proliferate on the Internet. In addition to the PCs, laptops, tablets and smartphones we all use every day, this will include sensors and monitors inside machinery, homes, buildings, vehicles and appliances that will allow us to control and repair devices as never before.

While this is all well and good, if not amazing, the IoT also presents security concerns. In the exuberance to connect everything in our lives, security is too often overlooked, resulting in devices that are generally defenseless.

These vulnerabilities, when exploited, can be tremendously costly in both lost dollars and the erosion of corporate reputations, brands and customer loyalty. The well-publicized Target breach could cost the company a billion dollars.[1] Hackers smuggled malware into the firm's point-of-sale (PoS) devices at its stores and reportedly stole 40 million credit card numbers and 70 million addresses, phone numbers and other personal information.

> The well-publicized Target breach could cost the company a billion dollars.
>
> *Charlotte Business Journal*

Soon after, Michaels Stores, the nation's largest crafts chain, reported that a security breach lasting eight months impacted three million of its customers.[2] Then a vulnerability with far greater implications was discovered lurking in most web servers. Called the Heartbleed bug, this liability potentially places at risk the personal information of anyone using some of the web's most frequented sites.[3]

[1] *Vomhof, John Jr., Charlotte Business Journal, February 3, 2014. Retrieved from http://www.bizjournals.com/charlotte/news/2014/02/03/targets-data-breach-fraud-cost-could-top-1-billion.html.*

[2] *Krebs on Security, April 17, 2014. Retrieved from http://krebsonsecurity.com/2014/04/3-million-customer-credit-debit-cards-stolen-in-michaels-aaron-brothers-breaches/.*

[3] *The Heartbleed Bug, April 29, 2014. Retrieved from www.heartbleed.com.*

One might believe that hackers predominantly attack devices that process credit card transactions. Why would they care about "dumb" sensors and probes? IoT malware has already been detected[4] and attacks on seemingly innocuous devices can pose risks. Their data can reveal a person's habits or a company's processes. By monitoring a thermostat, intruders can tell when a homeowner is away. By hacking into GPS-based devices, thieves can locate a truck and its shipment at any time. Hackers could also send falsified data upstream to misrepresent the status of critical systems. Perhaps more ominous, they can use IoT devices as gateways into corporate networks. Indeed, in such industries as financial, medical, retail, power and transportation, tampering with smart devices can have serious consequences.

Security has always been the shared responsibility of consumers, enterprise users, resellers and manufacturers. Yet many fail to see a smart thermostat or refrigerator as a vulnerability. All Internet-connected devices pose potential security risks. Any endpoint connected to the Internet is a viable target and can be commandeered to attack others.

Security Versus Ease-of-Use

Complicating matters is the tension between security and ease-of-use. Consumers demand devices that are simple to deploy and operate. Manufacturers oblige by configuring their products to work effortlessly, but with little or no security out-of-the-box. Users further undermine security by too often relying on simple or default passwords.

Moreover, IoT devices are ill-equipped to support firewall or anti-malware software. To keep them simple and inexpensive, they have limited processing power, RAM and flash storage. They are low-power devices with very specific functionality. They do not need much to work well.

All of these factors render IoT devices one of the most vulnerable assets connected to the Internet today. If the Internet of Things is to realize its potential, the industry must promptly address these risks. Etherios understands this and is at forefront of building the Internet of Things with the security it requires.

[4] *Thomas, Paul, "Despite the News, Your Refrigerator is Not Yet Sending Spam." January 23, 2014. Retrieved*

from http://www.symantec.com/connect/blogs/despite-news-your-refrigerator-not-yet-sending-spam

What Does IoT Security Look Like?

Security is complex with many moving parts. Good defense requires software updates, compliance monitoring and vigilance to deter attacks. Because IoT devices are abundant, highly distributed and small, the challenge is even greater. Etherios has identified the following requirements for device security.

Collective Management

Devices must be managed en masse for increased efficiencies. Managing devices individually is impractical and costly.

Safety in Clouds

Any solution should include a cloud-based platform, even if just as an option. Some customers collect and aggregate their IoT data themselves, but most lack the resources, expertise or inclination to build and staff an infrastructure for IoT data storage and processing.

A cloud platform offers these functionalities as a service. Any platform, however, must be hardened and offer complete redundancy for backups and availability.

Security as a Service

Device security management must be offered as a service to customers. Most enterprises will not want the bother and expense of securing their devices themselves, and consumers certainly will avoid the hassle. Both want the convenience of plug-and-play service. They will manage risk by entrusting their security to the professionals in managed IoT services.

Device Security as a Managed Service

Etherios is pioneering device security management, or device security-as-a-service. This service can be delivered as a one-time, consultative professional services engagement to help companies understand how to secure devices based on industry best practices. It also can be delivered as an ongoing managed service for proactive, centralized, security monitoring and management of all devices in a company's network. The managed service leverages Device Cloud by Etherios™, an award-winning multi-tenant, platform-as-a-service. Device Cloud aggregates device data, regardless of protocol or format, and performs data analytics to determine if any security weaknesses exist.

Consumers and enterprises will gain plug-and-play security and peace of mind through either of these Etherios services. Companies can continue to focus on gathering data from their devices while having their security monitored for them. Manufacturers will be able to offer IoT products that feature robust but affordable safeguards.

IoT solutions are Etherios' core competency. Etherios brings to bear expertise, experience and technologies that large enterprises, let alone small ones, would be hard pressed to match. With an advanced infrastructure and exhaustive security controls already in place, Etherios delivers managed device security services with efficiencies, scope and economy. Etherios' IoT solutions are engineered around the design philosophy of connecting devices securely, controlling them remotely and engaging them with business processes applications.

If Target's PoS registers had comprehensive, centrally managed security watching over them, the data breach might have been mitigated or prevented altogether.

Safeguard with a Complete Security Soution

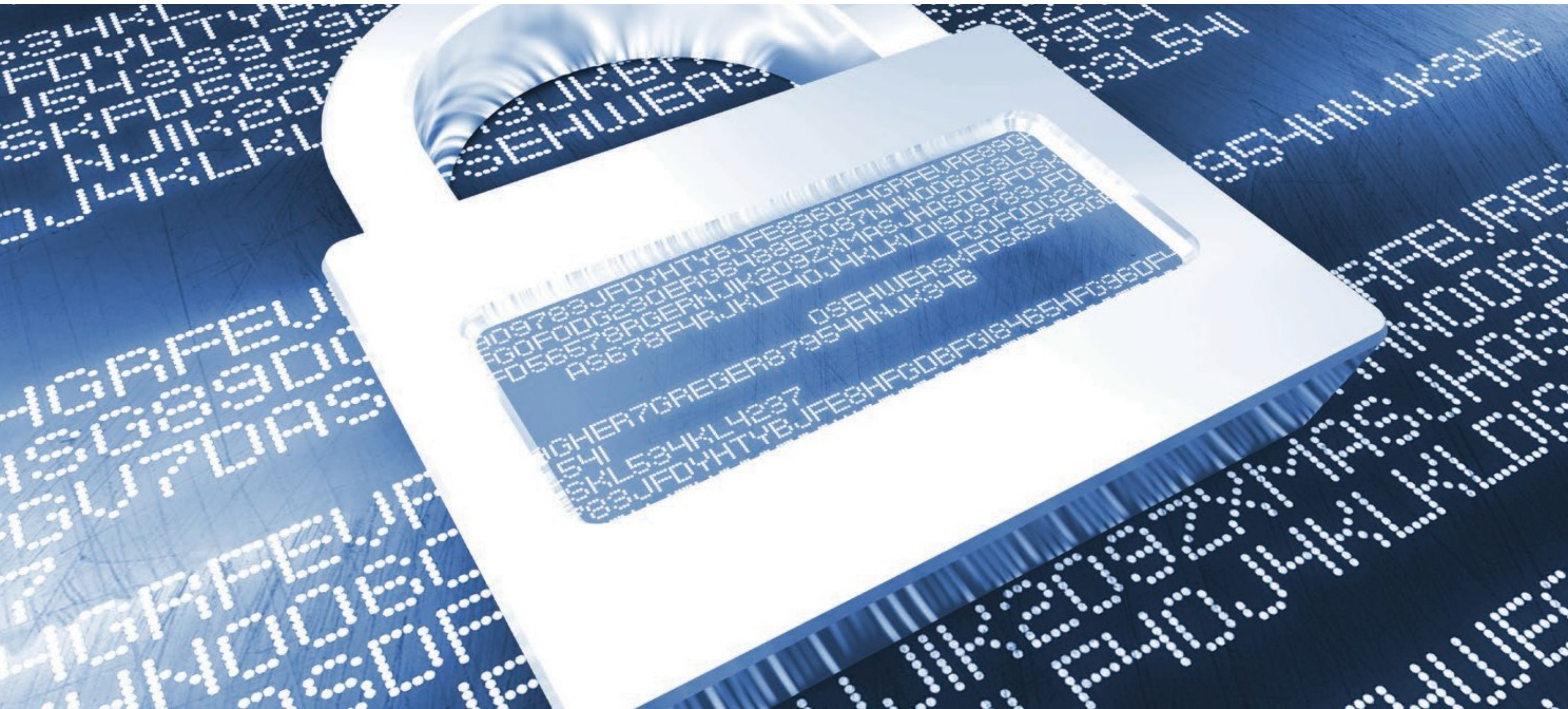
To mitigate risk, device security solutions need to holistically address recognized security needs and vulnerabilities. A complete security solution must deliver the following safeguards.

Centralized Logging

How would you know if a smart appliance is under attack? Full visibility into each device's activity is foundational to an IoT security posture. This includes when it was connected, disconnected, its IP address at these times, processor utilization, and if someone is tampering with the system. Centralized management and logging can reveal if any device, including a kitchen appliance, has been commandeered.

Visibility is achieved when the logs that each device issues are aggregated and monitored by security specialists who look for outliers that indicate questionable events. If such an event occurs, they can examine a device's log history to determine its activities and take appropriate actions.

Visibility is further enhanced when log monitoring correlates a device's IP address to a geographical location. This allows administrators to detect when a device suddenly logs in from a new location, prompting suspicions.



Authentication

Authentication is a fundamental security control. A device must confirm the identity of its target. The lack of verification invites threats like man-in-the-middle attacks, eavesdropping, data theft and device reconfigurations. Conversely, an application must confirm that it is receiving data from a trusted device. Well-proven technologies support authentication such as certificates, pre-shared keys and Secure-Sockets Layer (SSL) over HTTP, also known as HTTPS.

Encryption

IoT devices are not only susceptible to hijacking and brute-force attacks; they are also at risk for man-in-the-middle attacks when ne'er-do-wells inject themselves into the data stream between the device and the cloud. Data in transit is particularly vulnerable and must be encrypted. Negotiated public-key AES 256, for example, has shown to be impervious to non-brute force attacks.

The combination of authentication and encryption provides robust security over wireless as well as wired links. This is vital because many IoT devices access the Internet via wireless gateways.

Compliance Scanning, Remediation & Reporting

Compliance scanning detects when anyone tampers with a device or its configurations, as well as when new devices are brought online. Etherios' managed security service maintains a profile for each monitored device based on its firmware version, memory footprint and even a checksum of the firmware image itself. Etherios can determine when a profile has changed and a device is compromised, and then notify the customer proactively.

Etherios' managed security services can automatically take remediation measures. Auto-remediation reloads the correct configuration onto a compromised device, thwarting attempted hacks. For additional safety, devices even can be shut off, depending on pre-agreed upon policies.

To be effective, compliance scanning must occur continuously. Being certified for compliance once or twice a year is insufficient. To deter hackers who work every day, administrators must promptly know when they strike.

To deter hackers who work every day, administrators must promptly know when they strike.

Managed security services could have detected when Target's PoS devices had been corrupted and could have pushed down the correct firmware onto them. Had they become compromised again, auto-remediation would have again reloaded the proper firmware. This cycle would continue until administrators took further action. The ability to detect changes in devices and perform auto-remediation is a pillar of Etherios' core competency.

Centralized Device Patching

Any security posture is only as effective as its weakest link. Firmware is a weak link for IoT devices. IoT devices are designed to operate for many years – much longer than our computers. Yet their firmware is rarely updated, even though new security features and bug releases are typically available every six months. Even if a device is protected by other security measures, immutable firmware renders devices vulnerable to emerging threats and attacks.

A complete IoT solution includes the ability to update firmware and security patches remotely, which is most simply done through a managed security service. Etherios hardens deployments by pushing down updates as they are issued.

Intrusion Detection

Centralized logging detects intrusions. Without knowledge that somebody is trying to log into a device, there is no awareness of an attempted intrusion. It is akin to having a burglar set off the alarm in your house or business, but the system notifies no one.

> Without knowledge that somebody is trying to log into a device, there is no awareness of an attempted intrusion.

This lack of awareness was at the root of the Target breach. In the words of one security analyst, Target's security personnel "lacked the situational awareness to identify anomalous occurrences in their environment."[5]

Managed security services require the resources and expertise to achieve situational awareness by aggregating and mining data for abnormal or unwanted patterns. Solutions need to provide security information and event management (SIEM) functionality, enabling attacks to be detected and preventive measures taken.

Change Control

In addition to detecting unauthorized configuration changes, a managed security service should also push down configuration changes to devices as necessary. This capability simplifies the management of large numbers of IoT devices and ensures they are always current with the latest functionality and security settings.

Backup & Data Availability

A key aspect to protecting and securing data is ensuring the information is always available. Backup and data availability can be achieved by storing all device data—logs, profiles and readings—on a resilient cloud that routinely replicates data to ensure business continuity.

[5] *Bjorhus, J. (2014, March 12). McAfee report says Target cyber attackers used common methods. Minneapolis cyber-attackers-used-common.*

Star Tribune. Retrieved from http://www.mercurynews.com/business/ci_25322189/mcafee-report-says-target-

Standardizing the Internet of Things

Securing the IoT is not achievable by any one company. IoT safety demands the engagement of all stakeholders. Industry-wide standards are needed, particularly for authentication and encryption methods.

Unlike proprietary, enterprise-specific methods, standardized solutions have the support of broad communities of stakeholders. As vulnerabilities are detected, stakeholders quickly address them. When the day comes that manufacturers agree to standards, their devices will be secured more efficiently and economically to elevate the lowest common denominator.

Building a Safer Internet of Things

IoT is one of technology's fastest growing and most dynamic domains. It offers new applications, innovations and opportunities. Service providers however, must earn the trust of customers by ensuring the confidentiality, integrity and availability of services and data. The risks of inadequate defenses are well documented. Events like the Target breach undoubtedly remain vivid for many decision-makers.

IoT solutions that include a managed security service will enjoy a competitive advantage over those that do not. As users become aware of IoT vulnerabilities and as attacks on these systems persist, consumers and businesses will increasingly demand that their smart devices keep their data safe.

Etherios is leading the way to define best practices and deliver comprehensive device protection. Device Cloud already has over 175 different security controls in place. These account for such security frameworks as the Cloud Security Alliance (CSA) Cloud Controls Matrix, ISO27002's ISMS, NERC's critical infrastructure protection (CIP) guidance, Payment Card Industry PCI-DSS v2, as well as relevant HIPAA and NIST standards.

Combined with Digi's 25+ years of experience in machine connectivity as a device manufacturer, Etherios understands customers' needs. Etherios knows that world-class security demands daily vigilance, not just in monitoring devices, but also in anticipating and responding to always evolving threats. Etherios continually seeks new vulnerabilities and trends in security. Such rigor will make managed services compliant with demanding industry controls like PCI or HIPAA.

Etherios is committed to working with all stakeholders to make the Internet of Things safe and orderly. Etherios' security services will enable manufacturers to harden their IoT products without needing costly competencies and infrastructures, and will provide solutions for consumers who simply want things to work. Etherios is committed to an increasingly connected and informed world, but with ironclad privacy.

Is anything costlier than the lack of security?

cyber-attackers-used-common.

Key Takeaways:

- ✓ Securing the Internet of Things is a shared responsibility among all stakeholders.
- ✓ Collective device management, cloud-based infrastructure and active security management are key requirements for a secure IoT solution.
- ✓ Many of the recent breaches could have been remediated or prevented altogether if a security practice were in place.
- ✓ Utilize a managed service like Etherios' device security so you don't have to become an IoT security expert and can rest assured your devices and their data are safe.
- ✓ Talk to the experts at Etherios to develop a secure connected product strategy.

While every reasonable effort has been made to ensure that this information is accurate, complete and up-to-date, all information is provided "AS IS" without warranty of any kind. We disclaim liability for any reliance on this information. All registered trademarks or trademarks are property of their respective owners.

Contact us to realize your vision

PH: 888-287-2711
www.etherios.com

Chicago
190 South LaSalle Street
Suite 3010
Chicago, IL 60603

Dallas
5910 North Central Expressway
Suite 950
Dallas, TX 75206

Minneapolis
110 North 5th Street
Suite 400
Minneapolis, MN 55403

San Francisco
50 Fremont Street
Suite 2275
San Francisco, CA 94105

ETHERIOS
A Division of Digi International

/etherios @etherios in/etherios