Firewalls, Virus Scanners, and Other Similar Tools Are Not Enough

When It Comes to IoT Security, the Network Has an Obligation

01/22/2018 | Author/editor: Bernd König/Andreas Donner

More and more companies are using IoT-compatible devices, but in their rush toward digitalization they often forget about security. Sensors and IoT applications cannot provide any guarantees: A resilient, protective network is required.

The Mirai botnet has highlighted that there is also a dark side to the Internet of Things. Networked devices, whether sensors or actuators, can be easily enslaved and misappropriated via the IP protocol that links them together. Just over a year ago, the Mirai botnet was able to seize several hundred thousand devices and disrupt the Internet with the largest DDoS attack to date.

In total, the devices generated 623 Gbit/s of traffic, which overwhelmed and crippled specific websites. Barely a year later and the next Mirai wave — referred to as Reaper or IoTroop — is building. This wave exploits IoT software and hardware vulnerabilities, and is already responsible for more than a million infections.

However, the Internet of Things is now an indispensable part of our private and working lives. Around the world there are already more networked devices than people, and an estimated 50 billion IoT devices will be in service by 2020. As well as heightening the risk of increasingly refined attacks, a larger number of IoT devices also means a larger target.

While Mirai has still been attempting to hack passwords, the derivatives are exploiting known vulnerabilities and running complex attack scenarios. What's more, the new malware spreads from device to device and not from one central point, which means that the number of vulnerable networks that are linked to infected IoT devices is continually increasing. Companies need to act quickly to avoid jeopardizing their reputation and — most importantly — their existence.

IoT Devices Cannot Guarantee Security

It is crucial to raise awareness of the importance of security measures. In our enthusiasm for digitalization and amid the IoT hype, we frequently neglect to integrate defense mechanisms when implementing an IoT project. The actual devices are no real help, and many of those in networks have no security patches. Adequate defensive security functions are often unpopular and are usually ignored, as they tend to make devices less convenient to use.

This means that the network must take responsibility for security; a resilient corporate infrastructure will be faced with enormous challenges here. It has to manage the growing flood of data produced by IoT devices, while guaranteeing data integrity and availability alongside performance. It also has to identify previously unknown vulnerabilities — as well as new attack patterns — at an early stage, and provide protection against these. Trained specialists must monitor the complex security architecture, and they need to have an adequate budget for any upgrades that are required. This is on top of the efforts required to convince people that all this is necessary. Unfortunately, security in general and IoT security in particular are still not given top priority in the architecture for most infrastructures.

So let's imagine that security is the most important project in our IT department. What would the network need for it to be equipped to deal with attacks from IoT botnets?

No More "One Size Fits All" Policies for Security: Assessing Individual Risk

Before people start giving up at the thought of the mountain of tasks, the first step has to be carrying out an individual risk analysis, as not all companies need to fear a large-scale botnet attack. Evaluating threat data is useful here, as this sheds light on who has attacked the network and how. Security specialists in the company can use these results to design an individual security strategy that takes laws and industry-specific regulations into consideration. Although there is no such thing as complete protection against DDoS attacks, coming to grips with the IoT as part of corporate IT security will improve the chances of preventing a disaster.

Scalability and Knowledge Are Key

If you want to integrate IoT devices into your corporate infrastructure, you need to adapt the security measures to suit the new circumstances. The IoT generates huge quantities of data, which can quickly stretch company networks to their limits. But if you are the victim of a DDoS attack (because IoT devices are combined to create an illegal botnet, for example), you need to have sufficient scalability in your network to keep it from collapsing under the sudden data load.

This means you must be able to quickly expand capacities and maintain performance output at a stable level, so you can absorb the attacks and prevent downtime and data theft wherever possible.

This is where specialist staff and knowledge are required, if they are not already in place. Their task is to put the relevant infrastructure into practice. Although observing compliance and general industry standards is part of this process, it is far more important for those responsible to be aware of what the relevant threats are, and which vulnerabilities are likely to be exploited first. They also have to work continuously to identify and close any gaps, and ensure that the security structure remains up to date. New IoT devices have a high risk potential and must not simply be left to operate. Continuous analyses and patch routines can prevent gaps remaining undetected and being exploited mercilessly.

A Broadly Defined Defensive Strategy Is the Only Way to Maximize Security

The earlier a problem for the infrastructure is identified, the better the potential response. The first step in a defensive strategy is analyzing new applications in advance to establish their risk potential — which is particularly high, especially in IoT. The IT security concept must also provide a structure that has multiple lines of defense and covers prevention, analysis, and — ideally — automatic responses, from the perimeter of the network right through to the end point.

Early lines of defense at the perimeter of the network use innovative detection methods such as anomaly detection. This is where algorithms detect methods, including port scans, used by attackers to find out which ports are active and, consequently, which services are available. This extremely early detection stage requires knowledgeable IT staff, as the majority of the intelligence is applied in advance by analyzing and defining the algorithms and then by evaluating the automated alarms.

Over the years, and in response to the change in the threat level, we have also moved away from simply relying on the firewall or virus filter at the perimeter of the network. "Defense in depth" refers to a strategy that not only covers the outer borders of the network, but also incorporates all levels, layers, and vectors. This significantly increases the level of security because considerably more relevant areas of the network are monitored and analyzed on an ongoing basis, so their defenses are in place.

Security Must Be Faster than the Attacker

Worries about data theft and downtime that threaten the company are increasing — and rightly so. To prevent attacks on the infrastructure, a successful defense must be faster than the attacker, but this is almost impossible to achieve. Although predictive work in isolation seems less meaningful, it can still be a useful supplement.

New detection methods are constantly being developed, which make it possible to use indicators correlated from comprehensive analyses, and thus to identify and block threats from the Internet at an early stage. This is the approach that Akamai has chosen.

Bernd König. (Image: Akamai)

Article Source Link: https://www.ip-insider.de/das-netzwerk-steht-bei-iot-sicherheit-in-der-pflicht-a-675977/