Quick guide on how to make IoT your security enabler

November, 2017

There are two parts to this: the IoT platform and the devices that will connect to it.

1 **Apply cybersecurity from the very first development sprint.** Put an emphasis on threat modeling, as it will help you to prioritize your cybersecurity efforts and potential tradeoffs. Since your products will constantly become smarter, make sure that they are tamper-proof. This way you will ensure that your IPR won't get stolen, and that your product will not be used to attack any potential IoT cloud. Your IoT cloud, on the other hand, needs to treat every connected device as a potential threat as the connected devices are not always your own, unless you have a predefined trust available between device and the cloud (such as certificates).

Keep in mind that data is your gold. Ensuring data integrity will play a big part in your success, as AI and other machine learning technologies will utilize gathered data to provide you suggestions that will affect your business.

2 **Apply automated technologies to test your devices and IoT platforms.** Code analysis tools, vulnerability scanners, and Fuzzing products may be introduced as part of your DevOps to find potential security vulnerabilities at the earliest stages of product development. Additionally, you may harness your test automation platform with advanced security tests that simulate real attacks. The great part about largely known test automation frameworks is that most of the security testing tools mentioned earlier are actually available as plugins, which enables faster adoption and lower costs. Having a traditional process where security testing is performed at the very end of the product development cycle is comparable to gambling. If you are unlucky, the vulnerabilities found in your system will be resolved over the course of months of redevelopment and potentially delay your time-to-market plans.

3 **Don't forget privacy.** . In case you are not in the business of selling customers' personal data, try to avoid using it. This way you will minimize the risk of class action law suits and general PR risks that comes with data leakages. In case you do utilize customers' personal data, make sure that the consent policy is in place and that the customer understands the reason why his/her personal data is collected. At the end of the day, it comes down to value; if the gained value overcomes the potential drawbacks of sharing one's digital identity, customer will more likely let you collect information abut him/her. Just remember that even if your customers willingly share their private data with you, you are still responsible for keeping it safe, at least in the European Union. Also, customer has always the right to be forgotten. Having mechanisms in place to accommodate this request will save you a lot of effort in the long run.

④ **Make sure to establish a function with capability to maintain and update your products fast**, since someone else will buy/own your product and you will have very little control over it once it is out in the market. As the threat landscape evolves all the time, the capability of doing mitigation activities and software updates is crucial. In addition to the software update mechanism, make sure that you can revoke any device from accessing IoT cloud if needed, to avoid potentially greater damage in case of a security breach.

⑤ **Establish a function to detect and resolve cybersecurity incidents**, should one occur. Security monitoring will help you to evaluate the cybersecurity state of the devices out in the field and detect potential attacks against your products, be it digital or physical. Having such a function in place will increase your chances to react to potential security breaches before they hit the masses, thus minimizing incident impact. Obviously, your team will have to establish an incident response process that will include R&D and the communications department.

⑥ **Be proactive about your cybersecurity efforts:** tell your customers how you are taking care of cybersecurity throughout the lifecycle of your products. This will enable trust among your target customers and will work as a differentiating factor when competing against competitive offering.

/nixuoy
@nixutigerteam
/company/nixu-oy
sales@nixu.com
www.nixu.com

nixu
cybersecurity.

Nixu Corporation is a cybersecurity company. We work to improve our clients' cybersecurity in solution areas of Corporate IT, Digital Business and Industrial Internet. Our clients trust Nixu in projects where developing, implementing or assessing of information security is a must. We ensure the confidentiality of our clients' data, business continuity and ease-of-access to digital services through planning and mitigation of cybersecurity risks.