The Right Time to Hire a Security Analyst

December 14, 2020

Post-production is, by far, the most expensive time for a security analysis. And yet, companies continue to give short shrift to security, tacking it on as an afterthought instead of designing it into their products from the earliest stages.

A doll that understands what children say and **responds to them** seemed, in 2015, like a great idea — unless you were a security analyst.

Unfortunately for Mattel, security analysts seem to have been left out of the conversation until the toymaker's "Hello Barbie" had debuted on the market; security and privacy advocates had protested in the media; and the company's reputation had taken a major hit.

More recently, the video conferencing app Zoom had security issues, and **had to pay a settlement** to the U.S. Federal Trade Commission. Again, a security analyst, if consulted early in the application's design process, might have saved the company those fines as well as a lot of bad publicity.

These types of occurrences are all too common. Products get developed with little or no thought for security until something happens — and only then does the manufacturer call in the experts.

Is it any wonder that cybersecurity gets a bad reputation for being costly? **Post-production is, by far, the most expensive time for a security analysis.**

The best — and most cost-effective — time to consider security is during the budgeting process, before development even begins. It's also a great time for the board of directors to demonstrate its commitment to keeping the company and its customers safe from cyberattacks, especially when adopting a much-needed holistic approach.

And yet, companies and their boards continue to neglect security, tacking it on as an afterthought instead of designing it into their products from the earliest stages. Developers get the blame, but they're often working under time and budgetary constraints set by management and the board, who don't fully understand the need for "security by design."

Change is coming, however. Privacy and security regulations as well as increasing consumer awareness are already demanding that products be secure *before* coming on the market.

For instance, the **IoT Cybersecurity Improvement Act of 2020**, recently passed by the United States Congress and awaiting the President's signature, will require U.S. agencies to determine that internet-of-things devices conform to national security standards before connecting them to federal networks.

In the EU and Canada, certification for the *International Organization for Standardization/International Electrotechnical Commission* (ISO/IEC) 15408, *Common Criteria for Information Technology Security Evaluation*, requires a security analysis. Governments and organizations around the world mandate the use of Common Criteria-certified products only.

And the UK's Department for Digital, Culture, Media, and Sport has announced that it will impose security requirements on internet-connected devices sold to consumers as part of the government's "Secure by Design" program, which advocates that security be built into IoT products at the design stage.

Clearly, organizations already working with a security analyst when planning or designing their products will not only have the security edge over companies making similar products; they'll have a true marketable competitive advantage, as well.

How security analysis works

An effective product security analysis will examine your project at each step in the development process, from planning to design to development and beyond.

It begins with determining your enterprise's security objectives and assessing the risks to those objectives that your project might pose. Let's assume that your organization is making a wearable health monitoring device that transmits data to your healthcare provider, for instance. A security analyst will pinpoint potential vulnerabilities and risks:

- Which data will the device collect?
- How will it collect the information, and what happens to it after collection — is it analyzed on the device itself, or transmitted to analysis software in the cloud?
- Where does the analysis go, and where is the information stored?
- What barriers will be in place to prevent security breaches at every stage?

With many products containing millions of lines of code, errors, which are often subtle, can be extremely difficult to find. A security analyst can guide secure coding while it's being written, preventing mistakes and the product vulnerabilities they bring.

Even if your programmers write that code perfectly, errors can creep in from other sources. To work faster, developers may pull from libraries, which can contain flaws that may go unchecked. So, your own programmers' mistakes aren't the only ones you should be worried about.

Meanwhile, customers don't care where the code comes from — they want to feel safe using your product. A security analyst can scrutinize the library-sourced code to find and correct mistakes before they compromise your or your customer's systems, networks, and personal data.

Spotting and fixing errors is much easier and cheaper while a project is in progress. Think of it: what if, during construction of a new home or commercial building, engineers waited until the building was finished to test plumbing, electrical wiring, and other internal systems? In the event of a water leak, the faulty pipes would need to be excavated, and the damaged areas patched when repairs

were finished. The time and expense would be much greater than if testing had found the problem when the pipes were first laid.

In the same way, a security analyst will need more time to find and correct security flaws after a product is finished than if they had been involved from day one.

Bringing an analyst into your initial planning meeting allows them to ask questions and alert the development team and managers to potential problems so they can avoid making mistakes that could cost money down the road.

For instance, a security analyst most likely would have raised privacy, compliance and security concerns in the very first, conceptual discussions of the "Hello Barbie" doll. Perhaps managers would have decided not to make the doll at all — or, at least, would have been cognizant of issues that might arise later, such as privacy advocates' objections to having children's voices recorded and their conversations stored in a database for mining later. The toymaker could have taken steps to secure both the integrity and confidentiality of this data and proactively announced the measures to deflect criticism before it even began.

Security analysts could then have involved themselves in the design of the artificial intelligence software the dolls used -- and Mattel might have avoided the bad publicity it suffered when security vulnerabilities were uncovered shortly after the dolls' release.

Are developers to blame?

It's become fashionable to blame product designers and software developers for security flaws. This tendency is understandable: they are, after all, writing the code. But boards that scrimp on security during budgeting, C-suite executives who fail to make the case for funding security analysis, and pressure on developers to continually release new software and updates at the expense of security tend to be the real culprits.

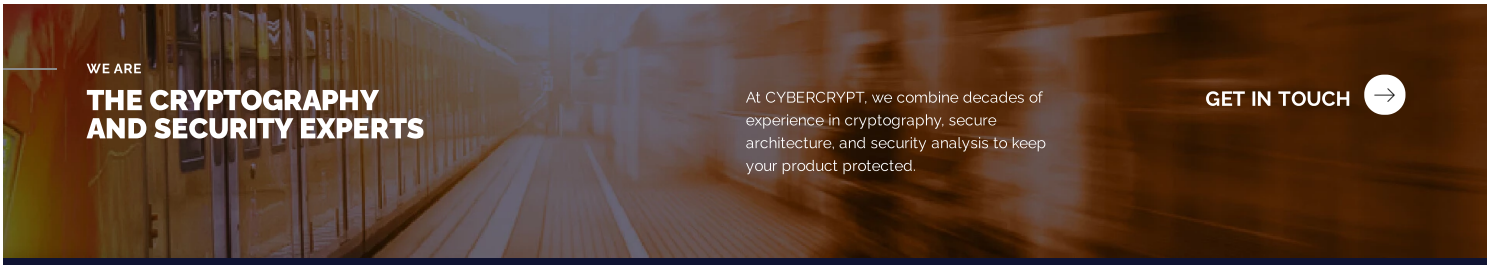
Increasingly, however, cutting corners on security means that insecure products are not going to make the cut. Regulators and consumers alike are coming down hard on tech, and insisting that software and digital products be inherently secure. Those that fail the test won't be released at all — unless their boards and management want to risk huge fines and possibly devastating consequences for the business.

The Payment Card Industry Data Security Standard (**PCI DSS**) requires companies to adhere to strict security guidelines aimed at protecting the privacy and security of credit and debit card transactions. Businesses that fail to meet the standards can lose their credit-card privileges, which could shut down e-commerce and in-person card payments. Medical applications must adhere to Health Insurance Portability and Availability Act (**HIPAA**) requirements. And so on.

After a fire has destroyed your property is not the time to buy fire insurance. After a product's release or deployment is not the time to think of securing it. Cost savings become lost opportunities as your un-launched product waits in limbo for approval, or your failure to achieve certification gives the edge to your competitors.

For years, boards and executives have considered security analysis "nice to have" for those who can afford it. Quickly, though, it's becoming a "must have" to stay in business — **no longer a luxury but a necessity; no longer a burdensome expense but a value enhancer.** And by starting your security analysis early in the process, you can lower your costs and boost your security — and overall —

BACK



CORPORATE HEADQUARTERS

Sankt Annæ Plads 13, st tv.
1250 Copenhagen, Denmark

info@cyber-crypt.com
+45 53737400