TAIVARA
Technology Innovation

Top 10 Security Best Practices

for

Digital Product

Overview

When developing and managing your digital product, solid security doesn't happen by accident. Product managers and owners that consider security from the start are able to assess their options and make informed choices based on the nature of their business and the sensitivity of the information being used.

Threats to data and digital products transform over time, but the fundamentals of solid security remain constant. Making sure that security is included in all phases of your product life cycle will not only reduce your cybersecurity risks, but ensure that you avoid costly surprises during product development and launch.

Following these Top 10 Security Best Practices will help you better develop a successful digital product.

1. Design for Security

Developing secure digital products isn't a new art. Over the past thirty years, security professionals have documented many principles that you can include during the design phase of your product. Including these principles will ensure you have a solid, secure product design.

Your team will also understand the importance of security and include it throughout the product life cycle. Security is not something added on. It needs to be designed into the product to have a chance at holding up against bad actors.

- Wikipedia's entry on "Secure by Design" is a good starting point: https://en.wikipedia.org/wiki/Secure_by_design

2. Understand your Data

Start by identifying the types of data you'll be handling (called "Asset Classification").

You'll also want to consider any regulatory or industry-specific best-practices regarding data protection. The most basic controls you'll put in place should include encryption of sensitive data during transmission (usually via TLS) and encryption of data while stored or "at rest."

Nothing is worse than finding out late in your product launch that you've not put sufficient work into understanding the requirements for handling sensitive information. It's worth thinking through the data that will drive your product and then making sure you have the proper security controls in place, including authentication, authorization, accounting, encryption, monitoring, and alerting.

3. Train Your Team

Make sure your team understands the importance of secure information & design in your product, and is trained on how to implement security properly.

This can be as simple as having developers trained on secure design and coding practices, or you may even want to implement regular code audits, app pen tests and other reviews for security.

It's important that developers are provided feedback on their code, and shown proper ways to make their code secure.

Formal training and certification of team members can be provided by a number of providers such as SANS, IANS and ISC2.

4. Engage Your Experts

Unless you're part of a startup or small company, odds are you have a person or team you can rely on to provide expert consulting on requirements for security.

Reach out to your Chief Information Security Officer, or lacking that, look to engage the people in your organization that are responsible for legal & regulatory compliance.

If you're in a startup or small company without internal resources then we suggest you include an external consultant in your budget.

One thing to note: most internal security teams are understaffed and sometimes overwhelmed, so don't be discouraged if they aren't able to be immediately responsive.

5. “Shift-Left” & DevOps

The basic goal with shift-left practices is to integrate testing earlier and into all phases of the product development life cycle. The concept is to identify and resolve potential issues well before the launch stage and even before you begin writing code for your digital product.

The term “Shift-Left” means including security in the “left” section of your product or project plan - the earliest stages. That helps address issues early and not put off until later in your product lifecycle.

Shifting left improves the security of your product, and also reduces the chance of costly delays or a failed launch due to security issues.

6. Follow Platform Guidelines for Security

In security, it's best to avoid reinventing the wheel. Leverage the work of others to save time, money and reduce risk at the same time.

Most platforms, such as iOS, Android, AWS, or Azure, provide detailed guidelines on how to leverage their security capabilities. This will not only save you time and money, but also help to make sure you're using best practices for the platform.

Often platform guidelines can help define how you'll implement many of the non-functional product requirements outlined in your system architecture.

If your platform doesn't provide for security, or the guidelines are lacking, you may want to consider looking at other approaches to developing your product.

7. Verify that Security Features Work

Much like any other feature that may be in your product, you'll want to make sure that security is working as planned. Examples of security features would be abuse cases, error handling / failing gracefully, and validating session flow.

Include testing of security capabilities in your testing plans, in addition to testing your core features.

This type of testing is especially important if your core features depend upon solid security, such as making sure that users of your product can't inappropriately access or modify other users information.

8. Test for Common Vulnerabilities

There is no way to make sure that your product won't have any vulnerabilities. You can, however, understand the most commonly known and easily foreseen vulnerabilities for your product during the design phase.

A great resource for identifying and prioritizing these common vulnerabilities is the Open Web Application Security Project (OWASP). They regularly identify common vulnerabilities, provide fee testing tools and even have a "Top 10" security risks: https://owasp.org/www-project-top-ten/.

If security is vital to your product, consider working with a security testing firm. These are security experts who can run your product through rigorous testing and identify vulnerabilities.

9. Make Sure Your Providers Implement Reasonable Security Measures

It's very rare these days to have a digital product designed, built, launched and maintained solely with internal resources.

You should make sure any vendors participating in your product (whether designers, developers, platform, partner or hosting providers) understand the importance of security to your product.

Make providers aware of your security requirements and verify that the services they provide will meet them. Make your security requirements explicit during requirements definition and include them in contract terms.

10. Maintain Security

Security isn't done once and forgotten. It should be woven into your product just like any other feature.

Having security-specific tasks as part of each stage of your product life cycle will ensure that you keep security in mind, and provide checkpoints where security is implemented, tested, and fixed (if broken). Starting early, with a focus on secure information and design, sets the stage for a lifetime of secure product.

To stay secure, you'll need to continue to invest in security as part of your product maintenance. Security is a very dynamic field. The longer your security stands still, the greater the risk for your product.

Contact Us

Taivara has the security expertise recommended in this document.

We'd love the opportunity to talk to you about the security of your next new digital product.

Call us today at 614-300-7374

TAIVARA

614-300-7374 hello@taivara.com **TAIVARA.com**