# Security Should Be Designed Into the Project

Security problems can become expensive when they are discovered after deployment. A development team should understand what information the application stores, who needs access, how users authenticate, which systems connect to the product, and what happens if an account is compromised.

KernDev approaches security as part of development rather than a final check. Our **cybersecurity service** capabilities cover security considerations across application development, infrastructure, access control, and system assessment.

For example, imagine a healthcare platform that stores patient information and allows staff members to access records. The system cannot treat every user as having the same permissions. A receptionist, physician, administrator, and system manager may need different access levels.

Our security specialists would examine authentication, permissions, encrypted data handling, session management, logging, backups, third-party integrations, and other relevant risks.

We use the same thinking for financial, ecommerce, HR, logistics, and enterprise systems. The specific risks differ according to the information and business process involved.

A realistic example is an employee management application containing payroll records. If every authenticated employee can access every record, the system may function correctly while still exposing sensitive information. Role-based access must be considered before the application is released.

Businesses should ask their development partner:

- What information will the application store?
- Who should have access?
- How are passwords and authentication handled?
- How are production credentials protected?
- How are security issues tested?
- How are logs and incidents handled?
- What happens when an employee leaves?
- How are third-party integrations secured?

Our recommendation is to involve security specialists early. Fixing a permission model during architecture planning is much easier than rebuilding a large application after launch.

Security is part of responsible software engineering, especially when an application handles customer, financial, employee, or operational information.