hakin9

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

VOL.15, NO. 07

SQL INJECTION ATTACKS

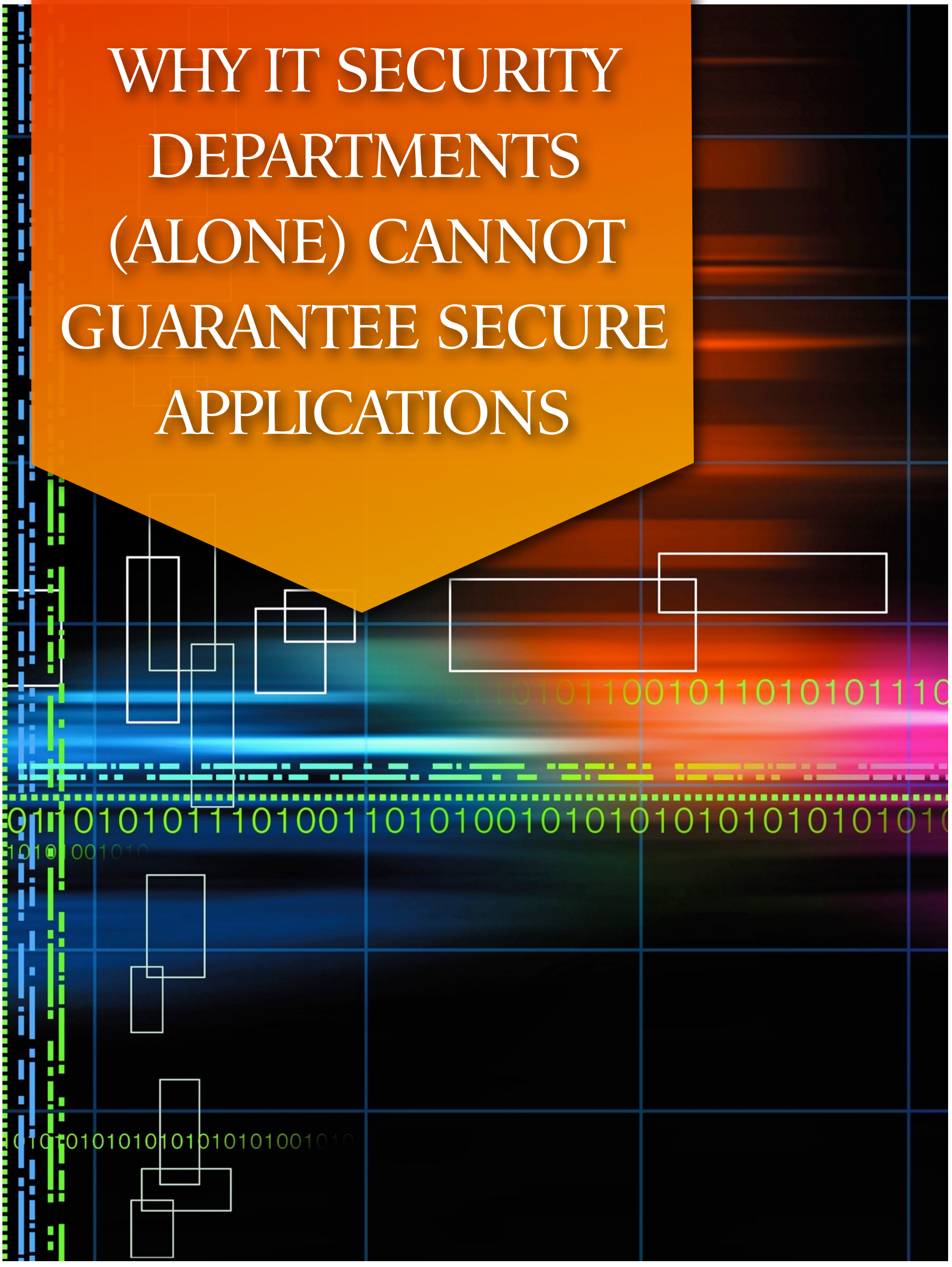
Reverse Shell and Privilege Escalation with SQL Injection

Time-based SQL Injection

A Detection and Prevention Technique on SQL Injection Attacks

AND MORE...

WHY IT SECURITY DEPARTMENTS (ALONE) CANNOT GUARANTEE SECURE APPLICATIONS



KLAUS HALLER

Klaus Haller is a Senior IT Project Manager with Business Analysis and Solutions Architecture knowhow with more than 15 years of experience in IT Consulting. Areas of expertise are data management, analytics, information security and compliance, and IT operations. Connect with him on LinkedIn https://www.linkedin.com/in/klaushaller/ and learn more about him on his personal homepage: http://www.klaushaller.net

Many business and IT professionals consider IT and information security as an incredibly important task – that someone else takes care of. Customers assume that the IT service provider is responsible. The business is sure that the IT department handles it. Software developers see the company's IT security department in the lead. Such assumptions and mind-sets are dangerous. Every team has to know its responsibility, act accordingly, and collaborate with the rest of the organization. Therefore, we provide a high-level overview of how various teams can work together to protect the organization's IT infrastructure, data, and information.

The Approach of Cloud Providers

Cloud providers frequently get unwanted press coverage. For example, The Hacker News writes on March 5th, 2020: "More than 200 million records containing a wide range of property-related information on US residents were left exposed on a database that was accessible on the web without requiring any password or authentication." [Lak20] This data was hosted on the Google Cloud – and this is not something global or local cloud providers want to be put into connection with or being made responsible for. Thus, they make it very clear what they are responsible for and what is the responsibility of their customers. AWS, for example, distinguishes between the security *of* the cloud and security *in* the cloud (Figure 1) [ASM]. Security of the cloud means that AWS ensures that its cloud services such as (managed) database services, load balancing services, or de- and encryption functionality are implemented correctly. It is the responsibility of the customer to put the various services together in a way that the overall application landscape and concrete software solutions are clear. This fundamental distinction between providers of single (security and other) services and the responsibility for the overall solution security is crucial when looking at the security architecture of concrete applications.

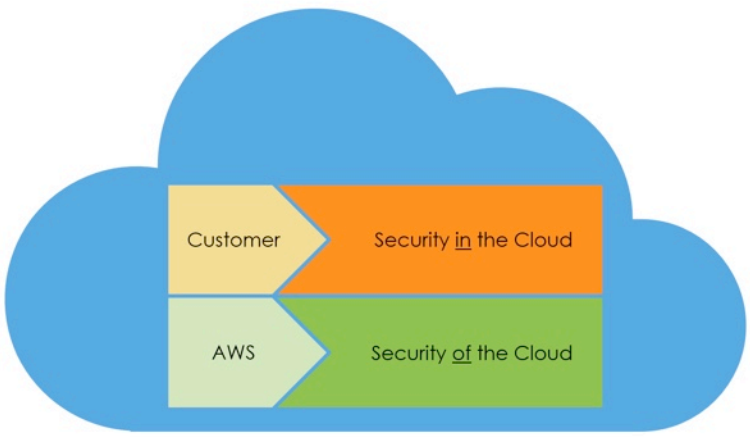


Figure 1: AWS Shared Responsibility Model for Security (simplified)

An Architectural Perspective

Concrete application architectures are more complex than the situation in diagrams and white papers of the cloud providers. Organizations outsource tasks to IT service providers; they use internally developed software as well as standard software. They have centralized services for databases and identity and access management whereas other tasks are taken over by the application teams. When IT service providers and outsourcing or consulting companies are involved, responsibilities are defined in the contracts. The division of responsibilities within an organization is often more challenging.

We elaborate on this aspect using the example of an internet-facing web application and discuss typical security components from an architecture perspective (Figure 2). The web application runs on a virtual machine with Linux. The application incorporates a (local) key-value store and stores larger amounts of data in a dedicated database instance. The database instance is hosted on the company's central database. Even with this initial set-up, various teams contribute to the application's security. First – and often overseen in stressful projects - the application developers must write secure code. They must know the OWASP-Top-10. They have to make sure to deploy security-related patches of the key-value software components – during development time and when the application is in production. They must implement authorization services properly. There must be no risky features such as exporting all clients to Excel for download. Neither the business, the application owner nor business analysts should demand and specify such features. When the software runs in a larger IT organization, the solutions architect is also responsible that the integration considers the security requirements. No security department or firewall can secure a messed-up application.

Second, when application teams rely on other teams (server operations, database services, etc.), they rely on the other teams securing these services properly. These teams can certainly rely on centralized shared security services for certain tasks such as virus scanning. However, such service teams have to take over all necessary security tasks related to their services that are not handled by other teams. Especially important is deploying the latest patches to software components and following the security best practices for their components.

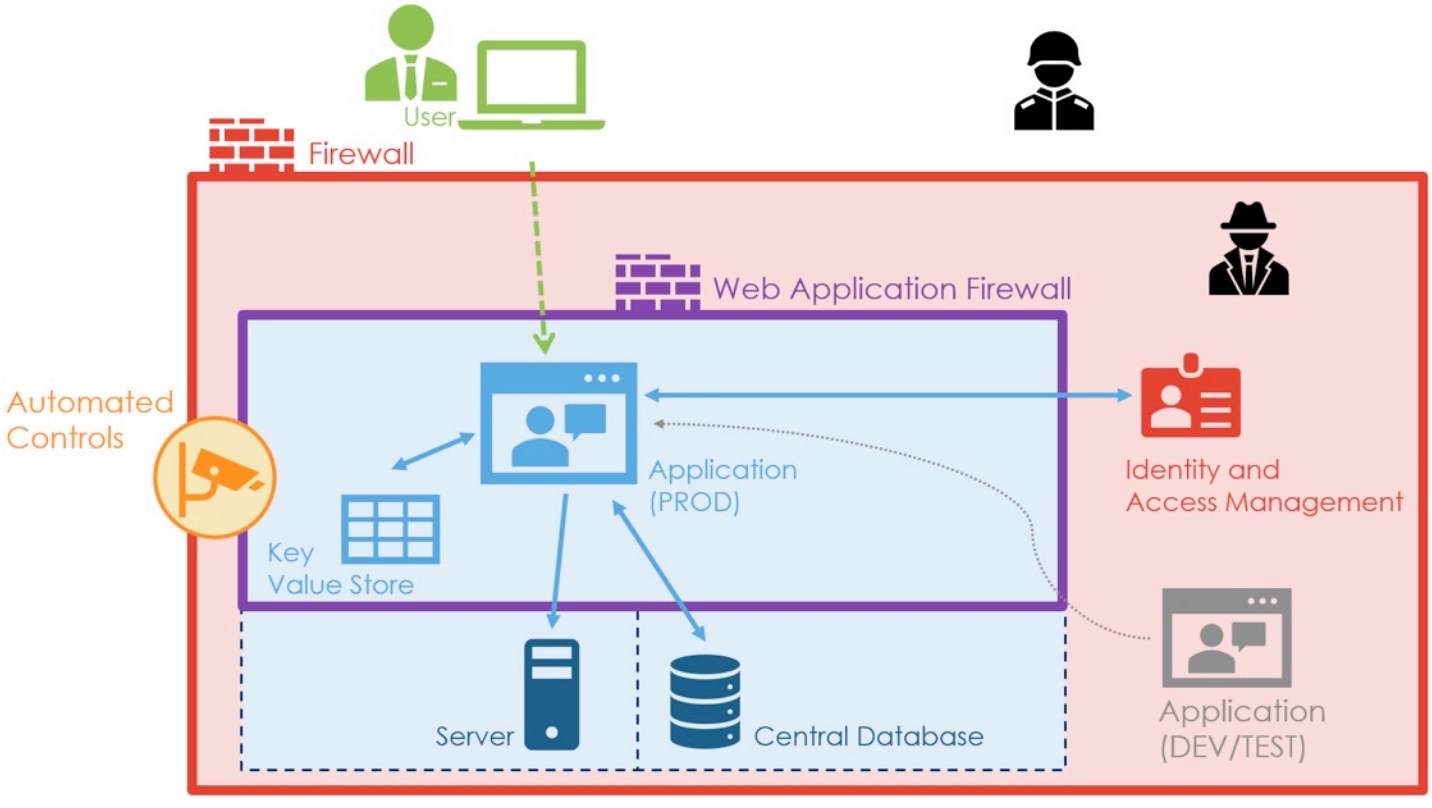


Figure 2: A Sample Security Architecture

When looking at the bigger picture, web applications are protected by a firewall at the company's network perimeter and between the various internal network zones. Furthermore, they are coupled with an identity and access management (IAM) solution to ensure that customers can use their normal password, or even benefit from single sign-on, and that all authorization aspects can be dealt with in one place. The perimeter firewall and the IAM solution have two aspects in common. First, the interaction between the team providing these services and the application team does not require much interaction and explanation. The application team sends a simple request: a list of ports that should be opened or a list of

roles to be created in the Microsoft AD. Second, the application teams have a direct benefit for the project when they send the request. The login gets easier for the users plus the firewall must be open. Otherwise, the application cannot be used. The application team has intrinsic motivation.

Internet-facing network zones are usually protected additionally with a web application firewall (WAF). They filter more granularly which requests are passed to the web application – and which ones are blocked. I know from my project experience that they are more complex to configure. A WAF team runs the software. The configuration of the WAF, however, requires intense collaboration between the application and the WAF teams. The application team has to provide expertise and invest time. The important point is that there is no direct disadvantage for the application project. The WAF team might simply configure the WAF for this application "wide open" and the application team can proceed with the project. However, this means that this extra layer of security is not set-up adequately. WAF is a technology or service that requires collaboration.

Finally, IT departments usually run various security applications and scanners as automated controls. Controls aim for detecting behavior and system configurations that pose a security risk: virus scanners, scanning for open ports, checking server configurations for missing patches, scanning outgoing email for sensitive data, etc.

Teams, Roles, and Responsibilities

While the previous section mentioned various teams, this section aims to put organizational questions in the front (Figure 3). An important aspect is to understand what central IT security tasks and teams exist. This is confusing for many engineers and managers in the business. There are two central tasks: security governance and shared centralized security services. Especially if they together form the IT security department, outsiders mix up these tasks often.

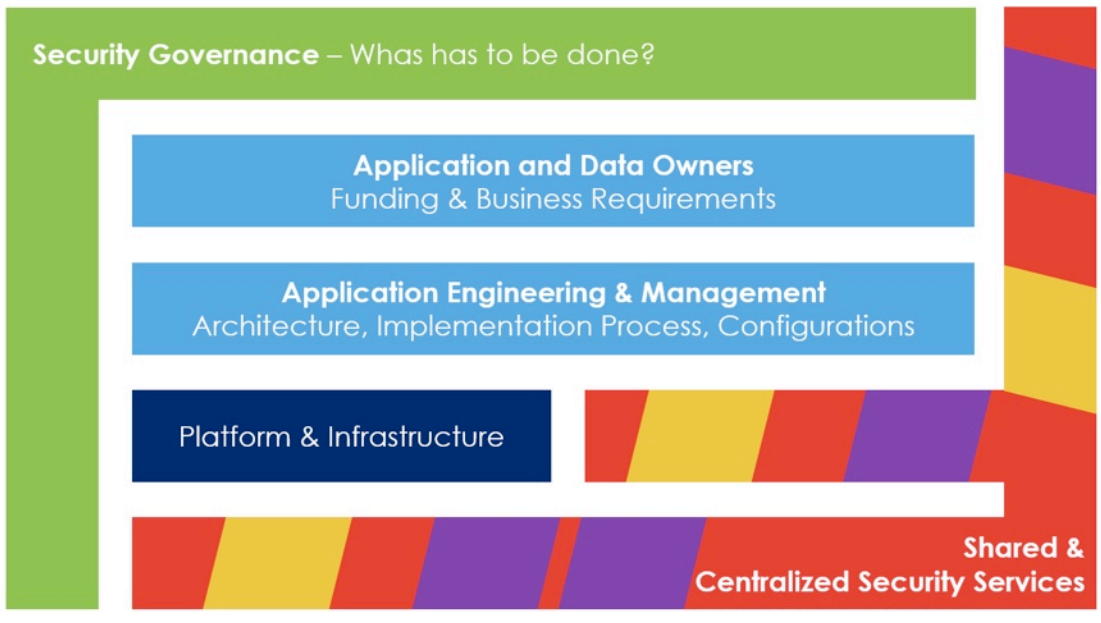


Figure 3: Teams involved in building secure IT application landscapes and IT solutions

The **security governance** team defines the security requirements applicable to the overall organization. It is a little bit like writing a wish list for Santa Claus. The security and governance team writes policies with procedural requirements (e.g., demanding penetration tests before going live with a web application), technical needs (all communication is

encrypted using RSA), or mandatory systems to be run (e.g., a data loss prevention solution). They are not involved in any service delivery. The rest of the company has to act as Santa Claus. They work on fulfilling the wishes respectively policies of this team. In many cases, security governance is one of the tasks of the Chief Information Security Officer.

Shared and centralized security services are especially important to fulfill these requirements. They provide solutions for well-established and infrastructure related topics, services that benefit many teams and applications in the organization, such as firewalls, or that automate controls, such as virus scanning or data loss prevention.

It might be confusing for engineers and the business to understand that even if security governance and shared and centralized security services together form the IT security organization, application management and engineering teams are still responsible for various security tasks. If the business owns and funds applications, the **application and data owners** are finally responsible and have to fund such activities. Plus, they have to make sure that the requirements (e.g., access control or export functionality) comply with the policies defined by the security governance team.

The **application engineering and management teams** architect the software solutions. They write (hopefully secure) code. In most cases, they invoke various other IT services and build on existing infrastructure. They (and no IT security organization) are responsible that their architecture is secure. They have to make sure that they use the central IAM or that they check file uploads for viruses.

Conclusion

The rise of the big cloud providers in combination with severe data leaks and an ever-increasing cyber-crime risk put security on the agenda of C-level executives. All too often, managers forget a famous statement from Bruce Schneier: “If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology.” Companies need technology to fight security but having a security team with the newest and best tools is not sufficient. Application maintenance and operations teams have to follow security best practices as well, build their applications on existing security building blocks – and collaborate with specialized teams to configure various security tools properly.

References:

1. [ASM] AWS Shared Responsibility Model, https://aws.amazon.com/compliance/shared-responsibility-model, last retrieved July 10th, 2020
2. [Lak20] R. Lakshmanan: A Massive U.S. Property and Demographic Database Exposes 200 Million Records, The Hacker News, March 5th, 2020