WIE SICHER IST IHRE IT-ARCHITEKTUR?

Machen Sie unseren Architektur-Check, und erfahren Sie, wie Sie neue Sicherheitsanforderungen besser unterstützen können!

Beim Stichwort „IT-Sicherheit“ denken wir zuerst an Hackerangriffe, Firewalls oder Penetrationstests. Dabei ist IT-Sicherheit ein deutlich größeres Feld. So kann unsere Systemarchitektur dazu beitragen, die Organisation vor Cybercrime und Industriespionage zu schützen, angefangen bei punktuellen Sicherheitslücken bis zu modernen Sicherheitskonzepten. Indem wir die Architektur sicher aufstellen, schließen wir wichtige Lücken, sorgen für die Sicherheit unserer Organisation und verhindern, dass Sicherheitsprobleme künftig überhaupt entstehen. Doch an welcher Stelle fangen wir an? Wo liegen die entscheidenden Hebel? Und wie können wir pragmatisch starten, ohne die Anwendung durch Sicherheitsbarrieren zu verkomplizieren? Unser Architektur-Check hilft Ihnen einen Einstieg zu finden – mit Analysen und einer individuellen, technologieunabhängigen Beratung.

Warum es bei der Security hakt

Während parallel zur Digitalisierung die Drohkulisse in puncto IT-Sicherheit anwächst, kommen die IT-Abteilungen hier oft nicht weiter. Dabei würden sie die nötigen Maßnahmen lieber heute als morgen umsetzen. Woran aber hakt es? Häufig erleben wir hier drei Gründe:

Grund 1: Sicherheit ist komplex und teuer

In kleineren Unternehmen ist die Anzahl der Systeme häufig dreistellig. In großen internationalen Unternehmen geht sie in die Tausende, auf diversen Infrastrukturen. Die IT hat es also mit vielfältigen Systemlandschaften und unterschiedlichsten Sicherheitsbedürfnissen zu tun. Schon kleinste Maßnahmen können massive Kosten und Risiken mit sich bringen.

Grund 2: Ressourcen und Erfahrungen fehlen

Die hohen Anforderungen an die IT-Sicherheit bringen viele IT-Abteilungen an ihre Grenzen: Manche haben die Systeme erst kürzlich übernommen. Andere müssen sich in das Thema Security noch einarbeiten. Wieder anderen fehlt die Zeit, sich zu den rechtlichen Regelungen und den neusten Technologien auf dem Laufenden zu halten.

Grund 3: Sicherheit schränkt Usability ein

Klar, Sicherheit ist wichtig! Doch wie verhindere ich, dass eine Anwendung ständig nach der Authentifizierung fragt oder umständliche Updates braucht, bis kein Mensch mehr Lust hat, damit zu arbeiten? Den Spagat zwischen Usabilty und Security scheuen wir und verlegen uns am Ende aufs Nichtstun.

Wie hilft der Architektur-Check?

Wo stehen Sie? Wo liegen Ihre Risiken? Wie können Sie Ihre IT-Architektur pragmatisch aber auch nachhaltig absichern? Um diese Fragen geht es bei unserem Architektur-Check. Nach dem Check sollten Sie an diese vier Punkte einen Haken machen können:

- Ich weiß, welche Sicherheitsmaßnahmen in meiner Architektur umgesetzt wurden.
- Ich weiß, an welchen Stellen ich meine Sicherheit noch weiter erhöhen könnte.
- Ich weiß, wie zufrieden meine Nutzer mit den eingesetzten Maßnahmen sind.
- Ich weiß, welche Sicherheitsmechanismen ich aus Usability-Gründen nicht einsetzen möchte.

Fact Sheet

Wie läuft der Architektur-Check ab?

1. Ist-Analyse

Anhand einer Checkliste gehen wir diverse Sicherheitsmechanismen und -techniken durch, von Anti-Malware bis Zugangssteuerung, von Backup-Strategie bis Patch Management. Dann vergleichen wir Ihren Status mit den aktuellen Standards, sodass Sie sich hier konkret verorten können.

2. Best Practices

Was macht eine gute Sicherheitsmaßnahme aus? Und was bezweckt sie? Gibt es Maßnahmen, auf die Sie eher verzichten könnten als auf andere? Sie erhalten von uns Best Practices zu jedem Punkt, der Sie interessiert.

3. Risikoanalyse

Nicht jeder Sicherheitsaspekt ist für jede Organisation relevant. Welche sind für Sie unverzichtbar? Wo liegen Ihre individuellen Risiken? Wir beziffern mit Ihnen die Auswirkung von Sicherheitslücken auf IT und Geschäft.

4. Next Steps

Gemeinsam planen wir Maßnahmen, die Sie konkret umsetzen können inklusive Risikoeinschätzung. Wir besprechen, was dafür genau zu tun ist und gehen die nächsten Schritte mit Ihnen durch.

5. User-Akzeptanz

Was denken die Anwendenden über Ihre Systeme? Wie groß ist das Sicherheitsbedürfnis? Zu wie viel Einschränkung sind sie bereit? Mithilfe von fachlichen Akzeptanztests bekommen Sie ein ehrliches Feedback.

Auf einen Blick

Rahmenbedingungen

- Dauer: Von einer Woche bis drei Monaten
- Kosten: Wir machen Ihnen ein individuelles Angebot
- Wer führt den Check durch? Je nach Thema binden wir Fachleute aus verschiedenen Bereichen ein.
- Was brauchen wir von Ihnen? Im Kick-off-Termin klären wir, was wir von Ihnen benötigen.

Inhalte

- Sie erfahren, wo Sie stehen
- Sie wissen, was möglich ist
- Sie können Risiken auch bei den Kosten einschätzen
- Sie planen mögliche nächste Schritte
- Sie erhalten Feedback von den Anwendenden

Ihre Vorteile

- Sie treffen Entscheidungen für Ihre individuellen Sicherheitsanforderungen
- Sie wissen, welche Kosten und Risiken Sie tragen können
- Sie profitieren von Erfahrungen aus Projekten in Ihrer Branche
- Sie bekommen Empfehlungen, die Sie direkt umsetzen können
- Auf Wunsch erhalten Sie Unterstützung auf dem weiteren Weg

Kontakt

Torsten Jaeschke
Senior Solution Architect

torsten.jaeschke
@opitz-consulting.com

OPITZ CONSULTING