„10 things I wished they'd told me!"

Sind Sie (sich) wirklich sicher? –

IT Security im Fokus

10 Tipps & Tricks zum Nachlesen

Vorwort

SEQIS, der führende österreichische Anbieter in den Bereichen Software Test und IT Analyse, gibt im Rahmen von kostenlosen Fachvorträgen rund um aktuelle Trendthemen 10 Tipps und Tricks zur Erfolgssteigerung in IT-Projekten und praktischen Umsetzung im Arbeitsalltag.

Auf den folgenden Karten sind die 10 Tipps zum Thema „Sind Sie (sich) wirklich sicher? – IT Security im Fokus“ übersichtlich zusammengefasst, sodass Sie diese jederzeit nachlesen können.

Einen ausführlichen Rückblick zur Veranstaltung sowie die Vortragsunterlagen zum Download finden Sie auf www.SEQIS.com.

1. Definieren Sie eine unternehmensweite Sicherheitsrichtlinie!

- Normen, Standards, Gesetze und Best Practices
- Detaillierungsgrad (gering → hoch)
- Persönliche Maßnahmen setzen

1. Definieren Sie eine unternehmensweite Sicherheitsrichtlinie!

Jedes Unternehmen braucht als Security Ausgangsbasis eine eindeutige Sicherheitsrichtlinie. Darauf stützen sich fast alle weiteren sicherheitsrelevanten Initiativen.

Gute Grundlagen für diese Richtlinie sind z.B. Gesetze (z.B. EU DGSVO), Normen (z.B. ÖNORM A 7700), Standards (z.B. PCI) oder Best Practices (z.B. OWASP).

Die unternehmensweite Sicherheitsrichtlinie definiert sowohl grob die generelle Bedeutung von Security im Unternehmen, den allgemeinen Umgang mit zu schützenden Daten, aber auch detailliert wie die Zugriffe auf Umgebungen (DEV/TST/PROD) geregelt sind oder wie der On & Offboarding Prozess im Detail umzusetzen ist.

Ein Tipp dabei: Versuchen Sie nur 1 (!) Richtlinie zu etablieren, diese sollte dafür jedoch stets aktuell und akkurat sein.

2. Unterstützen Sie Ihre Mitarbeiter mit sinnvollen Einschränkungen!

- Hürden werden kreativ (und unsicherer) umgangen
- Weniger ist mehr

2. Unterstützen Sie Ihre Mitarbeiter mit sinnvollen Einschränkungen!

Regeln müssen sein! Nicht umsonst beruht der erste Tipp auf der Definition von Sicherheitsrichtlinien. Diese Regeln führen sehr oft zu Einschränkungen der Mitarbeiter – ausführbare Dateien dürfen nicht per E-Mail versendet werden oder Passwörter müssen in (zu) kurzen Abständen wieder und wieder geändert werden. Die lokalen Schreibrechte sind auf wenige Bereiche beschränkt und USB-Geräte sind nicht oder nur eingeschränkt verwendbar.

Aus Security Sicht sind das auf den ersten Blick sinnvolle und verständliche Richtlinien, doch die Praxis lehrt das Gegenteil: Wird das tägliche Arbeiten durch große Hürden zu stark eingeschränkt, werden diese kreativ und unsicherer von den Mitarbeitern umgangen. Es tritt also der Effekt ein, dass die Sicherheit, trotz umfangreicher Regeln sinkt.

Hier gilt oft: Weniger ist mehr!

3. Security muss von Anfang an berücksichtigt werden!

- Security nachträglich zu integrieren ist aufwändig bis unmöglich
- Anforderungen speziell mit Blick auf Security definieren und prüfen

3. Security muss von Anfang an berücksichtigt werden!

Am Anfang jeder Software stehen die Anforderungen – funktionale und nicht funktionale. Um in der Analyse & Design Phase sicherheitsrelevante Anforderungen (oder Merkmale von Anforderungen) den notwendigen Stellenwert zu geben, müssen Sie besonders darauf eingehen: Erweitern Sie „Personas“ durch die Eigenschaft „Sicherheitsbewusstsein“. Aus den etablierten „6 thinking hats“ werden 7 → ein zusätzlicher „hat“ mit Fokus auf Security kommt hinzu.

Alle Anforderungen müssen natürlich den zuvor definierten Sicherheitsrichtlinien entsprechen, ein Review der Anforderungen in dieser Phase ist also angebracht.

Zusätzliche funktionale und nicht funktionale Anforderungen werden sich ergeben, wenn Sie die (auf Security bezogenen) Best Practices der eingesetzten Technologien und Architekturen berücksichtigen.

4. Definieren Sie Coding Guidelines und halten Sie diese ein!

- Disziplin und Commitment notwendig (besonders vor Deadlines/Milestones/...)
- Kaum technische Herausforderungen

4. Definieren Sie Coding Guidelines und halten Sie diese ein!

„I don‘t get your code“ – „Neither do I, but it seems to work“

Acht Beispiele für Coding Guidelines – diese sind auch in stressigen Zeiten, wie vor Releases oder Milestones, unbedingt zu beachten:

1. Code must be read- and understandable
2. Keep it small and simple
3. Minimize the attack surface area
4. Least necessary privilege
5. Obscurity is not security
6. Validate input and verify consistency
7. Don‘t trust (services, dependencies, ...)
8. Don‘t develop custom authentication and session management

5. Gehen Sie sorgsam mit Benutzerdaten um!

- Verwendung von (aus heutiger Sicht) als sicher geltende Algorithmen
- Passworte hashen, andere personenbezogene Daten (Sicherheitsfragen, Passwort Hinweise, ...) verschlüsseln

5. Gehen Sie sorgsam mit Benutzerdaten um!

Die Verantwortung der sicheren Aufbewahrung der Kundendaten liegt (ganz klar per Gesetz geregelt) beim Anbieter. Dementsprechend muss es auch in Ihrem Interesse sein, Benutzerdaten so zu persistieren, dass, im Falle eines Datenverlustes, die Auswirkungen minimal sind.

Dabei hilft: Benutzerdaten, die nicht im Klartext lesbar sein müssen (darunter fallen eindeutig Passwörter, aber auch Passwortfragen und -hinweise können so behandelt werden), werden mit kryptografischen Hash Algorithmen unidirektional verändert. Alle anderen zu schützenden Benutzerdaten (z.B. Kreditkarteninformationen) werden bidirektional verschlüsselt und können im Bedarfsfall wieder entschlüsselt werden.

Achtung: Es werden immer wieder Algorithmen als unsicher erklärt, sehen Sie also die Möglichkeit vor Ihre verwendeten Algorithmen einfach ändern zu können.

6. Forcieren Sie Länge und Eindeutigkeit bei Passwörtern!

- Komplexität allein hilft nicht
- Benutzung von Passwort Managern ermöglichen
- Optionale two factor authentication erhöht zusätzlich die Sicherheit

6. Forcieren Sie Länge und Eindeutigkeit bei Passwörtern!

„Mindestens eine Zahl, mindestens ein Sonderzeichen und ab und zu einfach mal ein neues Passwort“ (Bill Burr, 2003, *National Institute for Standards and Technology).*

14 Jahre nach dieser Definition eines (vermeintlich) guten Passwortes hat das *NIST* diese Aussagen revidiert, seien Sie Vorreiter und setzen Sie die neuen Empfehlungen bereits jetzt um:

1. Die Länge von Passwörtern ist deutlich mehr von Bedeutung als der verwendete Sprachraum: „*ein sicheres passwort“* (basiert nur auf Kleinbuchstaben und einem Sonderzeichen) ist deutlich (Faktor: 1 Million * 1 Million * 1 Million) sicherer als „*Pas_w0rT!*“, und obendrein noch einfacher zu merken
2. Verwenden Sie für jede Applikation/Portal ein neues eindeutiges Passwort

7. Security Issues findet man nicht nebenbei!

- Nur mit gezielten Tests und der Tester-Expertise ist das möglich
- Security-Status zyklisch mittels PEN Tests feststellen und Schwachstellen schließen

7. Security Issues findet man nicht nebenbei!

Beim Testen verhält es sich ähnlich wie bei der Anforderungsdefinition: Sicherheitsrelevante Anforderungen werden genauso wenig zufällig definiert, wie Security Issues durch einfache funktionale Test gefunden werden. Deswegen gilt hier auch der selbe Ansatz: Machen Sie bewusst Test Sessions mit Fokus auf Security z.B. auf sichere Authentifizierung und Session Management, XSS und SQL Injections oder auf korrekte serverseitige Validierung der Eingaben.

Organisieren Sie zusätzlich professionelle Penetration Tests: Dabei werden Ihre Architektur, Applikation bis hin zu Prozessen durchleuchtet, sicherheitsrelevante Schwachstellen identifiziert und dann mit Ihnen gemeinsam priorisiert und einer Lösung zugeführt.

8. Sichern Sie Ihre Systeme durch etablierte Appliances (IDS, IPS, UTM, usw.)!

- Test aller Updates auf (nicht) funktionale Sideeffects
- Fast Feedback durch gezielten Einsatz von Testautomation

8. Sichern Sie Ihre Systeme durch etablierte Appliances (IDS, IPS, UTM, usw.)!

Die Verwendung etablierter Appliances wie IDS, IPS, UTM, Firewall, NSM oder SIEM gehört heutzutage zum Standard – und das ist auch gut so! Doch eines gibt es zu Bedenken: All diese Appliances sind nur so gut wie diejenigen, die sie betreuen. Es ist also unbedingt notwendig dem Operations Team die notwendige Zeit für Know-how Aufbau und die Wartung der Regeln zu geben.

Systeme mit aktuellem Softwarestand und Patchlevel sind grundsätzlich weniger anfällig gegen Attacken als veraltete Systeme. Halten Sie also unbedingt alle Systeme up2date – und testen Sie nach jedem Update auf unerwartete negative Sideeffects. Schnelles Feedback bekommt man, wenn man die Software Testing Pyramide von Anfang an konsequent berücksichtigt.

9. Erstellen und testen Sie Ihren Data Breach Plan!

- Der Ernstfall muss gut vorbereitet sein und geprobt werden (RED Team)

9. Erstellen und testen Sie Ihren Data Breach Plan!

Der Data Breach Plan kommt im Ernstfall zum Einsatz und definiert konkrete Vorgehensweisen und Regeln – das heißt aber auch, dass er im Vorfeld erstellt, und unbedingt getestet werden muss. Ab dem Zeitpunkt, wo ein Datenleck bekannt wird, müssen jeder Schritt und jede Aktion mit Bedacht und Sicherheit gesetzt werden – das gelingt nur, wenn alle Beteiligten darin geübt sind.

Der Einsatz eines RED Team Assessments kann dabei helfen die bisher gesetzten Security Maßnahmen zu überprüfen und den Ernstfall so weit wie möglich zu simulieren.

10. Nehmen Sie Social Engineering ernst!

- Awareness schaffen durch Aufklärung, Workshops und Trainings aller Mitarbeiter

10. Nehmen Sie Social Engineering ernst!

Auch wenn wir technisch alles richtig gemacht haben, der Human Factor spielt beim Thema Security eine wesentliche Rolle: Die Tatsache, dass (laut einer deutschen Studie 2016) beinahe ein Drittel aller Passanten bereitwillig ihre Windows Benutzerdaten (inklusive Passwort) genannt haben, sollte die Alarmglocken schrillen lassen. Einzig die Tatsache, dass durch eine kleine Aufwandsentschädigung (in dem konkreten Fall Schokolade) die Quote auf fast 50% erhöht werden konnte, ist noch alarmierender: Mit rund 3 € kann man also alle getroffenen millionenschweren Investitionen zur Erhöhung der Sicherheit aushebeln.

Diesem Verhalten muss man als Unternehmen vorbeugen: Jegliche Art, die Awareness in diesem Bereich zu schärfen (z.B. durch gezielte Workshops), ist gut investiertes Geld.

11. Security muss aktiv betrieben werden!

- Nur darüber reden allein macht es nicht sicherer

11. Security muss aktiv betrieben werden!

Ich bin mir sicher: Wenn Sie diese Tipps in Händen halten sind Sie sich der durchaus bedrohlichen Situation bewusst. Jeder wird (früher oder später) oder wurde bereits Ziel einer Attacke. Wie man sich davor schützen kann oder die Auswirkungen auf ein sinnvolles Minimum reduziert ist in diversen Best Practices, Normen, Standards und nicht zuletzt in den vorigen „10 things“ beschrieben.

Fehlt also nur noch eine Kleinigkeit: Reden wir nicht länger über Security, sondern tun wir gemeinsam etwas dafür – besser früher als später!

Zusammenfassung

1. Definieren Sie eine unternehmensweite Sicherheitsrichtlinie!
2. Unterstützen Sie Ihre Mitarbeiter mit sinnvollen Einschränkungen!
3. Security muss von Anfang an berücksichtigt werden!
4. Definieren Sie Coding Guidelines und halten Sie diese ein!
5. Gehen Sie sorgsam mit Benutzerdaten um!
6. Forcieren Sie Länge und Eindeutigkeit bei Passwörtern!
7. Security Issues findet man nicht nebenbei!
8. Sichern Sie Ihre Systeme durch etablierte Appliances (IDS, IPS, UTM, usw.)!
9. Erstellen und testen Sie Ihren Data Breach Plan!
10. Nehmen Sie Social Engineering ernst!
11. Security muss aktiv betrieben werden!

Kontakt

Neusiedler Straße 36
A-2340 Mödling

Tel.: +43 2236 320 320 0
Fax: +43 2236 320 320 350

marketing@SEQIS.com
www.SEQIS.com

Folgen Sie uns:
www.SEQIS.com/de/blog-index
twitter.com/swtestiscool
facebook.com/SoftwareTestIsCool

Stand: November 2017