IT-Sicherheit

Sicherheitsprozesse

Prof. Dr. Dominik Merli, Prof. Dr. Lothar Braun

Sommersemester 2020

Hochschule Augsburg - Fakultät für Informatik

Beispiel: Sicherheit im Produktentwicklungsprozess

Eines Tages im Entwicklungsteam ...

Quelle: http://dilbert.com/strip/2011-05-17

Generelle Probleme

- Sicherheit meistens nicht im Mittelpunkt → niedrige Priorität
- Sicherheit oft eher eine Erweiterung als ein Basis-Feature
- Sicherheit kostet Geld
  - Personal und Ausbildung
  - Tools und Equipment
  - Prozesse und Wartung/Betreuung

Zwei positive Beispiele

- Microsoft
  - 2001/2002: Gravierende Sicherheitsprobleme
  - 2005/2006: ”Trendsetter” im Bereich Software-Sicherheit
- Siemens
  - 2009/2010: Schwachstellen führen zu Stuxnet Vorfall
  - 2016/2017: Vorreiterrolle bei industrieller Sicherheit
- Aber wie haben diese Firmen die Wende geschafft?!

Es geht um Qualität

- Sicherheit ist ein Qualitätsmerkmal

- Überschneidet sich / konkurriert mit …
  - Funktionssicherheit (Safety)
  - Datenschutz (Privacy)
  - Zuverlässigkeit
  - Performance
  - Kompatibilität
  - Langzeit-Nutzung
  - und vielem mehr …

- Hohe Qualität wird meist durch etablierte und optimierte Prozesse erreicht!

Proaktive Sicherheitsprozesse

Zwei typische Prozesse, um Sicherheit zu schaffen

- Sicherer Produktentwicklungsprozess
  - Betrifft Hersteller von Software und Hardware, aber auch Integratoren
  - Security-by-Design: Sicherheit muss von Anfang bedacht werden
  - z.B. Umsetzung der Norm IEC 62443-4-1

- Informationssicherheitsmanagementprozess
  - Betrifft IT und Informationsmanagement in diversen Unternehmen
  - Fokus auf Unternehmensabläufe, Systeme und Schnittstellen
  - z.B. Umsetzung der Norm ISO 27001

Zuständigkeiten und Management

- Verbindliche Zusagen vom Management nötig!
  - Finanzielle und personelle Ressourcen
  - Zielsetzung und Zeitrahmen

- Typische Fragen
  - Wer ist für Sicherheit verantwortlich?
  - Wo sind Prozesse und Anforderungen definiert?
  - Welche Richtlinien und Standards müssen eingehalten werden?
  - Welche Verpflichtungen haben externe Partner?

Schulung und Aufklärung

- Grundlegende Security Awareness
  - Basis-Wissen für Verhalten im Alltag
  - Betrifft alle Mitarbeiter bis hoch zur Geschäftsführung

- Spezifische Experten-Ausbildungen
  - z.B. Secure Coding Schulungen für Entwickler
  - z.B. Netzwerkverkehranalyse Training für Administratoren

- Sicherheitswissen auf aktuellem Stand halten
  - z.B. jährliche Schulungen
  - z.B. kontinuierliche Zusammenarbeit mit externen (Forschungs-)Partnern

PDCA Zyklus (auch Deming-Kreis)

- Plan
  - Aufstellen von Sicherheitsanforderungen und -konzepten
- Do
  - Umsetzung von Sicherheitsmaßnahmen und -konzepten
- Check
  - Test der Wirksamkeit der implementierten Schutzmaßnahmen
- Act
  - Ggf. Beseitigung von Mängeln und Beginn des Zyklus von vorne

Bedrohungs- und Risikoanalyse

Motivation

- Erster Schritt hin zu strukturiertem Sicherheitsprozess!

- Wozu?
  - Identifikation von relevanten Bedrohungen
  - Transparente Darstellung für Management
  - Priorisierung nächster Schritte und Maßnahmen auf Basis der Ergebnisse

- Wie?
  - Produkt-/Unternehmens-/Architektur- und Sicherheitsexperten gemeinsam
  - Oft in Workshops organisiert
  - Regelmäßige Aktualisierung, z.B. jährlich

Vorbereitung

- Informationen zum Analyse-Gegenstand, z.B. IT-System oder Produkt
  - Architektur-Bild
  - Geschäfts-/Betriebsmodell
  - Anwendungsfälle
  - Rechtliche Rahmenbedingungen
  - Externe Abhängigkeiten (explizites/implizites Vertrauen)

- Workshop-Teilnehmer
  - Experten aus verschiedensten Bereichen einladen
  - Multidimensionale Sicht äußerst wertvoll!

Wer sollte mitmachen?

- Im Fall eines Produkt
  - z.B. Produkt-Manager, Architekt, Entwickler, Tester, Wartungsingenieur, Support-Mitarbeiter, Digitalisierungs-Abteilung, ...
- Im Fall eines IT-Systems
  - z.B. IT-Administrator, IT-Anwender, Support-Mitarbeiter, Abteilungsleiter, ...
- Immer beteiligt: Sicherheitsexperten und ein Moderator!

Vokabular

Schutzziele für Daten und Systeme

Vertraulichkeit (engl. confidentiality)

- Kein Zugriff auf System/Datum ohne Erlaubnis

Integrität (engl. integrity)

- Änderungen am System/Datum ohne Erlaubnis nicht möglich

Verfügbarkeit (engl. availability)

- Ordnungsgemäßer Zugriff auf System/Datum kann nicht behindert werden

Schutzziele in Verbindung mit Benutzer-/Geräteidentitäten

Authentizität (engl. authenticity)

- Datum/Objekt stammt tatsächlich von einer spezifischen Identität

Verbindlichkeit (engl. non-repudiation)

- Durchführung einer Aktion mit einer spezifischen Identität kann im Nachhinein nicht abgestritten werden.

Schutzziele für personenbezogene Daten

Anonymität (engl. anonymity)

- Daten und Aktionen können nicht auf eine bestimmte Person zugeführt werden

Pseudonymität (engl. pseudonymity)

- Daten und Aktionen können zu einem Pseudonym zurück verfolgt werden, aber die Person hinter dem Pseudonym bleibt unbekannt

Schützenswerte Güter und Vertrauen

Schützenswertes Gut (engl. asset)

- Digitales oder reales Gut, das es zu schützen gilt

Vertrauen (engl. trust)

- Überzeugung, dass etwas unter best. Umständen sicher ist

Schwachstellen und Verwundbarkeiten

Schwachstelle (engl. weakness)

- Systemschwäche, die das System verwundbar machen kann

Verwundbarkeit (engl. vulnerability)

- Schwachstelle, die tatsächlich ausgenutzt werden kann, um Schutzmechanismen eines Systems zu umgehen

Werden häufig synonym verwendet! (auch in dieser Veranstaltung)

Bedrohungen und Risiken

Bedrohung (engl. threat)

- Potentielle Ausnutzung einer Schwachstelle/Verwundbarkeit

Bedrohungswahrscheinlichkeit (engl. threat probability)

- Wahrscheinlichkeit, dass eine Bedrohung tatsächlich eintritt

Bedrohungsauswirkungen (engl. threat impact)

- Konsequenzen, die eine eingetretene Bedrohung hätte

Risiko (engl. risk)

- Verbindung aus Wahrscheinlichkeit und Auswirkung einer Bedrohung

Bedrohungs- und Risikoanalyse – Detaillierter Ablauf

Durchführung

- Gemeinsames System-Verständnis schaffen
  - Architektur, Eigenschaften und Abhängigkeiten werden klar
- Schützenswerte Güter identifizieren
  - Sammlung der wichtigsten Assets in einem Produkt/System
- Mögliche Angreifer(-gruppen) identifizieren
  - Sammlung aller Personen(-gruppen), die als Angreifer in Frage kommen
- Bedrohungsszenarien finden
  - Sammlung verschiedenster Bedrohungen im Anwendungskontext
- Bedrohungsszenarien und Risiken bewerten
  - Bewertung von Wahrscheinlichkeiten, Auswirkungen und Risiken)

Gemeinsames System-Verständnis schaffen

- Fragen
  - Welche Komponenten sind involviert und welche Schnittstellen haben sie?
  - Welches Geschäfts-/Betriebsmodell wird verfolgt?
  - Welche Abhängigkeiten gibt es zu externen Firmen/Produkten/Systemen?
- Aufwand für diese Phase sollte auf keinen Fall unterschätzt werden
- Grobes Konzept sollte vorab erstellt werden, sonst evtl. langwierig

Schützenswerte Güter identifizieren

- Fragen
  - Welche Assets gibt es im vorliegenden System/Produkt?
  - Welche Schutzziele haben diese Assets?
  - Welchen Stellenwert haben die Assets untereinander?

- Fokus auf kritische Teile, die z.B. für Geschäftsmodell, fehlerfreien Betrieb, Knowhow-Schutz, etc. relevant sind

Mögliche Angreifer(-gruppen) identifizieren

- Fragen
  - Welche Personen sind im normalen Betrieb involviert?
  - Wer könnte Motivation haben das System anzugreifen?
  - Haben auch unbekannte/außenstehende Personen Interesse anzugreifen?
  - Sind breit angelegte Angriffe relevant (Kollateralschaden)?

- Hineinversetzen in die Personen(-gruppen) kann sehr hilfreich sein

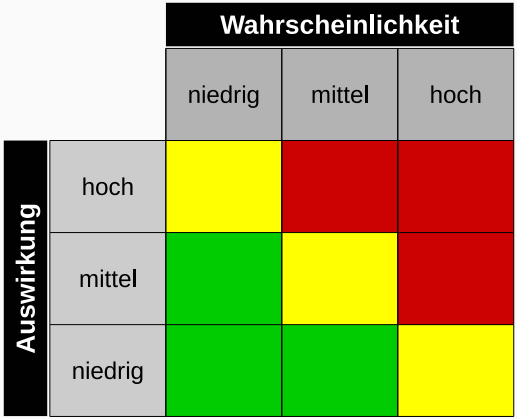
Bedrohungen finden

- Frage: Was könnte an welcher Stelle schief gehen?
- STRIDE Bedrohungen
  - Spoofing → Authentizität
    (Vorgeben etwas/jemand anderes zu sein)
  - Tampering → Integrität
    (Etwas manipulieren, das nicht manipuliert werden darf)
  - Repudiation → Verbindlichkeit
    (Bestreiten etwas getan zu haben)
  - Information Disclosure → Vertraulichkeit
    (Jemandem Informationen zugänglich machen, die er nicht kennen darf)
  - Denial of Service → Verfügbarkeit
    (Die Ausführung von etwas verhindern)
  - Elevation of Privilege → Autorisierung
    (Jemandem erlauben etwas zu tun, das er nicht darf)

Bedrohungen bewerten

- Eintrittswahrscheinlichkeit
  - niedrig
  - mittel
  - hoch
- Auswirkung
  - niedrig
  - mittel
  - hoch
- Risiko = Wahrscheinlichkeit x Auswirkung

Risiko-Matrix



- Ermöglicht Priorisierung nächster Schritte auf Basis der identifizierten Risiken

Risiken adressieren

- Abschwächen
  - Schutzmaßnahmen integrieren
  - Auswirkungen reduzieren
- Eliminieren
  - Funktionalität/Feature entfernen
- Verschieben
  - Zu anderen System-/Produktteilen
  - Zum Kunden
  - Zu externen Partnern
- Akzeptieren
  - Falls Abschwächung zu teuer/aufwendig
  - Falls Eliminierung und Verschiebung nicht möglich
  - Managemententscheidung

Gibt es noch Fragen?

Reaktive Sicherheitsprozesse

Incidents und Vulnerabilities

- Zwei typische Sicherheits-Probleme, die im Alltag auftreten können
  - Incident = Vorfall/Zwischenfall
    → Angriff auf laufendes System
  - Vulnerability = Verwundbarkeit
    → System/Produkt/Infrastruktur hat ausnutzbare Schwachstelle

- Hinweis oft von Externen
  - Sicherheitsforscher
  - Penetration Tester
  - Privat- oder Geschäftskunden
  - Bösartige Angreifer

- Im Folgenden: Fokus auf Vulnerability Response, Incident Response aber ähnlich

Warum sich um Vulnerabilities sorgen?

- In jedem System/Produkt sind Fehler
  - Selbst beim Einhalten eines proaktiven Sicherheitsprozesses
  - Menschen machen Fehler

- Es wird immer neue Schwachstellen geben
  - Fortschreiten der Sicherheitsforschung
  - Entdeckung neuer Klassen von Angriffen
  - Probleme, die bei Entwicklung/Inbetriebnahme unbekannt waren
  - Zunahme der Stärke von Angreifern und deren Tools

Wie wird Vulnerability Response organisiert?

- Etablierung eines Vulnerability Response Prozesses
  - Bei großen Unternehmen z.B. durch Security Response Center

- Prozessschritte (nach Howard & Lipner)
  1) Bericht/Auftauchen der Schwachstelle
  2) Verstehen und Bewerten der Schwachstelle
  3) Erstellung eines Patches
  4) Pflege der Beziehung zum Entdecker der Lücke
  5) Testen des Patches
  6) Vorbereiten von Informationen zur Schwachstelle
  7) Veröffentlichung der Information und des Updates
  8) Erkenntnisse für die Zukunft

Prozess zur Behandlung von Vulnerabilities

Bericht/Auftauchen der Schwachstelle

- Kontaktdaten sollten öffentlich bekannt sein
  - Es muss einfach sein, Schwachstellen zu melden
- Überwachen relevanter Mailing-Lists
  - z.B. exploit-db.com und seclists.org/fulldisclosure
- Innerhalb von 24 Stunden aktiv werden
  - Antwort an Entdecker, Anstoßen des internen Prozesses, etc.

Verstehen und Bewerten der Schwachstelle

- Sehr unterschiedlicher Detaillierungsgrad
  - Kompletter Proof-of-Concept bis hin zu vagen Hinweisen
- Bewertung der möglichen Auswirkungen wichtig
  - Sicherheitsexperten zusammen mit Produktspezialisten
- Benötigte Ergebnisse
  - Richtigkeit der berichteten Schwachstelle
  - Ausmaß und Auswirkungen, mögliche Gegenmaßnahmen
  - Einfluss anderer Faktoren auf Ausmaß/Auswirkungen

Erstellung eines Patches

- Sobald Schwachstelle komplett verstanden wurde
  - Läuft parallel zu Pflege der Beziehung zum Entdecker
- Muss folgende Ergebnisse erzielen
  - Elimination der entdeckten Schwachstelle
  - Elimination von verwandten Schwachstellen
  - Keine Einschränkung der Produkt-Funktionalität
- Könnte auch für andere Produkte relevant sein
  - Andere Produktversionen, -konfigurationen, -sprachen, etc.

Pflege der Beziehung zum Entdecker der Lücke

- Vertrauensvolle Beziehung wichtig
  - Perspektive/Situation des Entdeckers einbeziehen
- Prozess transparent gestalten
  - Entdecker auf dem Laufenden halten, z.B. wöchentlich
  - Persönlich und freundlich kommunizieren
- Arbeit des Entdeckers wertschätzen
  - Nicht als Gegenspieler betrachten
  - Evtl. Patch frühzeitig mit Entdecker teilen
  - Evtl. Praktika, Empfehlungen, etc. anbieten
  - Evtl. sind Bug Bounty Programme möglich

Testen des Patches

- Zeit ist ein entscheidender Faktor
  - Kritische Updates so schnell wie möglich verteilen
- Tests haben hohe Priorität
  - Bestätigung, dass Lücke tatsächlich geschlossen wurde
  - Versuch, Auswirkung auf Produkt zu minimieren
- Zusätzliche Test von Externen hilfreich
  - Spezielle Kunden mit bestimmten Vereinbarungen
  - Experten, die die Schwachstelle gefunden haben

Vorbereiten von Informationen zur Schwachstelle

- Security-Artikel für IT-Spezialisten
  - Detaillierte Informationen zur Schwachstelle
  - Mögliche Gegenmaßnahmen und Umgehungsmethoden
  - Hilfreich für Client/Server Wartungsmanagement
- Informationen für Endnutzer
  - Kurze Beschreibung mit Empfehlung zum Update
- Weitere Informationen
  - Warnungen, falls es kein Update gibt
  - Kernfragen und Antworten für Presse

Veröffentlichung der Information und des Updates

- Veröffentlichung des Updates
  - Auf bekannten Websites
  - Durch automatisierte Update-Verteilung
- Freigabe der Informationen zur Schwachstelle
  - An IT- und Security-Experten
  - An Kundenservice und Vertrieb
- In regelmäßigen, vorhersehbaren Terminen
  - z.B. an einem speziellen Tag jeden Monat
  - Gleichzeitige Verteilung des Updates an alle

Erkenntnisse für die Zukunft

- Ursache der Schwachstelle
  - Reflexion auf allen Prozessebenen
  - Empfehlung für die Vermeidung ähnlicher Probleme
- Suche nach weiteren Schwachstellen
  - Verbesserung noch vor Auslieferung des Produkts
  - Nicht darauf warten, dass Externe weitere Lücken finden

Gibt es noch Fragen?