DRK Kliniken Berlin

Rahmenbedingungen für einen Security-Check von IT-Systemen

Ausgangspositionen und Vorgaben für eine externe Beurteilung / Prüfung von Sicherheitseinrichtungen und IT-Systemen

Michael Thoss
DRK Kliniken Berlin
Leiter Zentrale Dienste Organisation und IT

Ausgangspositionen

- Zyklische Maßnahme der IT
- Auftrag der Unternehmensleitung
- Bestandteil des Risikomanagements (z.B. aus KonTraG oder auch Basel IV ff

Risikopotentiale

- Die bestehenden Risikopotentiale der IT-Systeme definieren sich auf unterschiedlichen Ebenen:
- Anforderungen an die Systeme (z.B. durch Hersteller-Vorgaben)
- Technologiebedingte Schwächen (Mangel am Produkt bereits Herstellerseitig z.B. Betriebssystem)
- Konfigurationsbedingte Schwächen (Mangel bei der Einstellung des Produktes, z.B. Administrationsfehler)
- Organisationsbedingte Schwächen (Mangel bei der Nutzung des Produktes, der Zugänge z.B. öffentliche Passwort auf „Post-It“)

Ausgangsbasis: Realistische Bedingungen

- Den vorgenannten Schwächen wird nicht nur systemseitig entgegen gewirkt, sondern auch mittels organisatorischer Maßnahmen.
- Auf dieser Basis muss eine qualifizierter Test auch die tatsächliche externe Ausgangslage berücksichtigen.
- **Daher wird ein dreiteiliger Test empfohlen:**
  - **A.** Externe Penetrationsversuche ohne Bereitstellung nicht-öffentlicher Informationen wie z.B. IP-Nummern und Einwahltelefonnummern (Zero-Knowledge-Konzept)
  - **B.** Bedingte Freigabe von Informationen mit Geheimhaltungsstatus, z.B. RAS-Einwahlnummer (Vertraulichkeitsverpflichtung)
  - **C.** Interner Penetrationstest unter Zuhilfenahme von interna wie Anmeldungen etc.
- Im Ergebnis sind diese Stufen auch unterschiedlich zu würdigen, um eine realistische Gefährdungssituation zu beurteilen

Ergebnisprognose (Auszug 1)

- In einigen Bereichen sind „negative“ Ergebnisse im Vorfeld absehbar. I.d.R. leiten diese sich aber aus Anforderungen / Vorgaben der Applikationshersteller ab und sind daher leider oftmals betriebsnotwendig. Beispiele hierfür sind u.a.:
  - ftp und snmp-Zugänge auf Server- und Netzwerkkomponenten für Remoteservices oder Systemüberwachung der Hersteller
  - Lokale Administrator Rechte auf Front-Ends ohne die die Applikationen nicht funktionieren
  - Allgemeine Zugriffsrechte auf System-Server (z.B. für Updateroutinen, zentrale Formulare)
  - Freie Ports am Firewall zur Bedienung spezifischer Applikationen (Services aber auch medizinische Studien)

Ergebnisbericht / Anforderungen / Ableitung

- Gewichtung der Risiken (Standard)
- Differenzierung zwischen 0-Knowledge und Knowledge darstellen zur Spezifikation Risikogewichtung
- Keine als „vertraulich“ vermittelten Informationen im Bericht ausweisen

Hintergrund: Bestimmte vertrauliche Informationen werden auch unternehmensintern als Grundlage der Security nicht bekannt gegeben.

Testrisiken

- Erfahrungen aus vorangegangenen Tests:
  - Netzwerkscan und Versuchszugriffe führten zum Absturz von Kassenautomaten und damit Beeinträchtigungen der Patientenversorgung (Telefonkarten, Abrechnung, Guthabenauszahlung)
  - Serverpenetrationsversuche führten zu Beeinträchtigungen einzelner Server-Cluster
  - Absturz der Remoteservices machte vor-Ort-Einsätze notwendig
- FAZIT: Prüfung auf Ausgrenzung bestimmter Bereiche oder Prüfung auf erzielte Verbesserungen bei gleichem Risikopotential

Gewichtung Testergebnisse

- Professionelle Sicherheitsheitstester finden grundsätzlich Schwächen in IT-Systemen. Dies ergibt sich bereits aus den systemimmanenten Schwächen die Herstellerseitig verursacht sind und wird ggf. durch Konfigurations- und Administrationsfehler begünstigt / nicht kompensiert.
- Für eine sachgerechte Gewichtung reicht aber nicht die Differenzierung der Ergebnisse nach niedriger, mittlerer oder höherer Gefährdung (Standardvorgehen) sondern es muss ebenfalls Berücksichtigt werden, in welchem Umfang interna für die Zielerreichung verwendet wurden
- Ohne diese Gewichtung können ggf. notwendige finanzielle Aufwendungen nicht beurteilt werden

Übersicht der IT-Systeme

In der Folge werden die einzelnen Gefährdungspotentiale systemspezifisch abgebildet.

ACHTUNG: Interne Informationen sind im Rahmen der Sicherheitskonzepte nicht zur Veröffentlichung freigegeben!

Internetpräsenz

- Interne Internetpräsenzen bedeuten ein höheres Risiko, da die Systeme für Dritte zu erreichen sein müssen. Daher ist die Bildung einer DMZ im Zusammenhang mit den Firewall-Systemen notwendig
- Im Unternehmen haben wir uns aus Sicherheitsgründen gegen eine selbst verwaltete Präsenz entschieden und unsere Webpräsenz extern gehostet (Provider)

Internetpräsenz (Ausgangsbasis Test)

- Einzige Information an den Tester/Penetrierer:
  - Domainname
  - Innerhalb der Präsenz: Mailadressen (Option)
- Testinhalt:
  - Angriff auf die Domain
  - Versuch des Zugriffs auf weitere Funktionen zum Beispiel:
  - Mailverkehr aus und in die tatsächlichen Klinikdomains und –bereiche (falls zu ermitteln…) verfolgen oder darüber Zugriffe versuchen
- Risikobeurteilung

Neues Potential: Webportale

- Auf Grund der Vorgaben der Unternehmensleitung und der Anforderungen des Datenschutzes mussten Portalsysteme in im Hause erstellt und im Rahmen einer DMZ platziert werden. Der Service erfolgt extern.
  - Dies entspricht nur bedingt Konzepten der IT im Rahmen der Sicherheit, ist aber oftmals nicht anders lösbar.
  - Ein Penetrationstest ist Angesichts der dort verfügbaren Personendaten und des neuen Systems sinnvoll.
- Testbedingungen:
  - Weitergabe der Domainadressierung
  - Penetrationsversuch
- Risikobeurteilung

Internetverkehr / -nutzung

- Die Systeme des Unternehmens sind mehrfach geschützt:
- Firewall-System
- Virenscanner und Contentfilter auf Site-Basis
- Zugangsberechtigungen für die Internetnutzung werden ausschließlich personenbezogen vergeben

Internetverkehr (Ausgangsbasis Test)

- Testbedingungen (Stufe B, **nicht** A):
  - Ggf. Bekanntgabe der Firewall-IP-Adressierung (Dies entspricht bereits der Weitergabe besonders geschützter Daten, die sich extern nicht ohne weiteres ermitteln lassen, allerdings im Zusammenhang mit vorhergehenden Teststufen eigentlich erkannt werden müssen)
  - Penetrationstest (sofern nicht in Stufe A möglich)
- Risikobeurteilung unter Berücksichtigung der ggf. freigegebenen interna

Virenschutz

- Mail- und Dateiverkehr im Unternehmen wird auf folgenden Stufen gesichert:
- 1. Genereller Scan aller ein- und ausgehenden mails Richtung Internet und externe Kontakte (am zentralen Ein- und Ausgangspunkt)
- 2. Genereller Scan aller ein- und ausgehenden internen mails (an jedem Standort, zwischen allen Standorten)
- 3. Genereller Scan aller Files am Front-End mittels zusätzlichem Front-End-Scanner (zur Absicherung ggf. freigegebener Disketten- oder CD-Laufwerke)

Rufnummernblöcke (TK-Anlagen)

- Im Rahmen von Penetrationstest sollten auch immer Rufnummerblöcke oder gezielt einzelne Rufnummern geprüft werden. Beispiele für entsprechenden Bedarf sind:
- Ermittlung eventuell unbekannter Modems
- Überprüfung individueller Servicemodems an z.B. technischen Einrichtungen
- Generelle Prüfung der Kommunikationslandschaft
- Achtung: Auf Testzeiten achten ggf. Rufnummerblöcke ausgrenzen (Vermeidung Belästigung)

RAS-Zugänge

- Das Unternehmen verfügt über Remote-Access-Servicezugänge für Software- und Systempartner
- Der Schwerpunkt der Sicherheit liegt auf Organisation: Keine „öffentlichmachung“ der Zugangsnummern und auf Technologie: Routerkonzepte, Sicherheitsabfragen und Passwortschutz ggf. Rückrufoptionen und IP- bzw. Anruferregistrierung / -authentifizierung

RAS-Zugänge (Ausgangsbasis Test)

- A. Versuch des Testers/Penetrierers in Eigenleistung einen RAS-Zugang ausfindig zu machen
  - Bedingt unter realistischen Bedingungen die Anwahl aller in Frage kommenden Telefonnummern…
- B. GGf. Freigabe einer Einwahlnummer zum Penetrationstest falls ersteres scheitert
- Risikobeurteilung unter Berücksichtigung A bzw. B als Ausgangsbasis

DRK Kliniken Berlin

Einwahloptionen Nutzer

- Das Unternehmen verfügt im Rahmen des WAN VPN (IPSec) über eine Remoteeinwahlfunktion auf ISDN-Basis
- Der Zugang wird sowohl über die Technologie des Carriers als auch über das Unternehmen abgesichert (z.B. RADIUS-Server)
- Schutzmechanismen basieren somit wiederum auf Organisation (Geheimhaltung Nummer) als auch auf Technologie (RAS-Einwahl, Sicherheitsserver, Authentifizierung)

DRK Kliniken Berlin

Einwahloptionen Nutzer (Ausgangsbasis Test)

- TEST auf Grundlage der Rufnummer
- Penetrationstest
- Risikobeurteilung

DRK Kliniken Berlin

Netzwerkkomponenten

- WAN und LAN(s) des Unternehmens basieren zum überwiegenden Teil (größer 98%) auf Switch-Technologie
- Die Sicherheit liegt damit deutlich über der klassischer HUBs
- Restbestände sind auf Grund der nur sukzessive finanzierbaren Gerätewechsel noch bedingt vorhanden

DRK Kliniken Berlin

Netzwerkkomponenten (Ausgangsbasis Test)

- Interner Netzwerkscan (nach Abstimmung)
- Penetrationsversuch
- Risikobeurteilung

- Im Rahmen der Risikobeurteilung ist ggf. festzuhalten, ob Zugriffe auf Netzwerkkomponenten bereits im Rahmen der vorhergehenden Teststufen gelungen sind, oder erst nach Überlassung von Zugangsmöglichkeiten, z.B. durch Bekanntgabe „nicht-öffentlicher“ Informationen

DRK Kliniken Berlin

Primärserver KIS

- SUN-Systeme
- Betriebssystem Sun UNIX-Solaris und Datenbank Oracle
- (Konfiguration der Server durch den Hersteller)
- Konfiguration der Server nach den Anforderungen der KIS-Applikation
- Konfiguration verschiedener Remotezugänge (über Firewall) auf Grund der Servicebedürfnisse der Sw-Hersteller-Administration- und Serviceinheiten an den Systemen im Interesse des störungsfreien Systembetriebs (z.B. ftp-Erlaubnis, sql-net, etc.)

DRK Kliniken Berlin

Zugangsberechtigungen

- Stufe 1:
  Netzwerkzugang: Persönliche Accounts (z.B. Verwaltung, Arztdienst) und Gruppen-Accounts (z.B. Stationspersonal, Arbeitsgruppen Funktions- und Leistungsstellen). Organisatorischer Bedarf zwingend notwendig
- Stufe 2:
  Applikationszugang KIS: Ausschließliche persönliche Accounts, keine Gruppenaccounts (aus Dokumentationspflicht EPA)
- Stufe 3:
  Subsysteme: Teilweise unterschiedliche Accounts mit unterschiedlichen Rechten aus Vorgaben der Datenverantwortlichen oder Systemhersteller

Primärserver KIS (Ausgangsbasis Test)

- Allgemeiner Zugriffsversuch mittels Standardpasswort (Netzwerkanmeldung)
- Penetrationsversuch
- Risikobeurteilung
  - Ergebnis: Härtung der Systeme wird empfohlen

Sekundärserver (z.B. Exchange / intern)

- Zentraler Exchangeserver für ein- und ausgehende Nachrichten in Zusammenhang mit Internet-Kontakten
- Verteilte Exchangeserver zur Standortversorgung und standortübergreifenden Kommunikation
- Ausgangsbasis Test:
  - Interne Prüfung der Systeme unter (ggf.) Bereitstellung notwendiger Zugriffsrechte auf das allgemeine Netzwerk
  - Penetrationsversuch
- Risikobeurteilung

Sekundärserver (Subsysteme)

- Zum Beispiel für:
- SQL-Datenbanken
- IntraNett
- Abteilungs-Subsysteme
- File- und Printservices, Softwareverteilung
- e-learning

- Scanning im Rahmen der Netzwerkuntersuchung
- Systembeurteilung, Penetrationsversuch
- Risikobeurteilung

Sekundärserver (Abteilungshoheit)

- Selbstverwaltete Server ohne (regelmäßige) Mitwirkung der IT finden sich im Rahmen gewollter organisatorischer Lösungen in verschiedenen Abteilungen.
- Ein Systemprüfung ist ggf. gezielt zu beauftragen
- Zu diesen Systemen und den aktuellen Sicherheitsstati kann die IT i.d.R. keine Stellung nehmen. Sofern solche System im Rahmen der Tests benannt werden, muss ggf. über eine qualifizierte Lösung entschieden werden. Grundlage hierfür liefern die Ergebnisse.

Zugangsberechtigung für Test (Standard)

- Nutzung einer Standardzugangsberechtigung, z.B.
  - Allgemeiner Arbeitsplatz (Anmeldung beschränkt auf bestimmte Arbeitsplätze) – „teilöffentlicher Bereich“
  - Anmeldung Sonderdienste
  - Anmeldung Verwaltungsarbeitsplatz

PC-Arbeitsplatz für Test (Standard)

- Nutzung eines Standard-Arbeitsplatzes für den internen Penetrationstest
- Auf dem Standardarbeitsplatz sollten die Zugriffe auf Diskettenlaufwerke und CD-ROM sowie auf das BIOS (und USB) grundsätzlich ausgeschaltet sein.
  (Ausnahmeregelungen in Einzelfällen antragsbasiert)