# TECHNICAL REPORT

## Gegenmaßnahmen zu bestehenden Bring Your Own Device Risiken

M.Sc. Jeron Mehl
mehl@fzi.de

# Inhalt

# Einleitung

Im Rahmen eines Industrieprojektes am FZI Forschungszentrums Informatik wurden mit dem Ziel der Umsetzung einer Bring Your Own Device Strategie in einem weltweit agierenden Unternehmen Gegenmaßnahmen für bestehende Risiken von Bring Your Own Device erarbeitet. Die Risiken sind einer Veröffentlichung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) entnommen [1]. Je nach Einstufung des einzelnen Risikos kann zwischen Stufen unterschiedlicher Intensität der Gegenmaßnahme gewählt werden. Auf diese Art und Weise ist die Wahl der Gegenmaßnahme sehr flexibel im Hinblick auf eine Einstufung des Risikos.

Der vorliegende Technical Report ist wie folgt aufgebaut: in Abschnitt zwei werden die einzelnen Risiken der Veröffentlichung des BSI nochmals aufgegriffen und in wenigen Worten beschrieben. Zwei gewählte Beispiele verdeutlicht jeweils das einzelne Risiko. Weiterhin werden die Gegenmaßnahmen ausführlich beschrieben. In diesem Zusammenhang wird auch auf die Einstufung der einzelnen Risiken eingegangen. Abschnitt drei beinhaltet eine Zusammenfassung und beendet den Technical Report.

## Risiken und Gegenmaßnahmen

Im Folgenden werden die einzelnen Risiken der Veröffentlichung "Mobile Endgeräte und mobile Applikationen: Sicherheitsgefährdungen und Schutzmaßnahmen" des Bundesamts für Sicherheit in der Informationstechnik kurz erläutert und mit einzelnen Beispielen verdeutlicht.

### *R1 – Manipulation*

Durch das Zerstören oder Modifizieren von Hardware kann das Endgerät ganz oder teilweise außer Betrieb gesetzt werden. Dies kann je nach Endgerät zu verschiedenen Einschränkungen des Benutzers führen. Möglich wäre neben dem Entfernen oder Zerstören von Hardware auch das Hinzufügen von Hardware, sodass Abhörgeräte oder Ähnliches verbaut werden könnten.

***Beispiele:***

- Datenverlust durch Zerstörung eines USB-Sticks
- Unterbrechung der Datenverbind

| Risiko | Gegenmaßnahme |
|---|---|
| **hoch** | Private Endgeräte dürfen nicht genutzt werden, da über die Hardware keine Absicherungen getroffen werden können. |
| **mittel** | Endgeräte werden durch Siegel geschützt, sodass Benutzer erkennen können, ob das Endgerät geöffnet wurde. Das Endgerät wird von einer Prüfstelle innerhalb des Unternehmens geprüft und (ggf. erneut) versiegelt. |
| **gering** | Der Mitarbeiter wird lediglich über die Gefahren informiert. |

### *R2 – Gerätemerkmale*

Durch Zugriff auf die Gerätehardware können Systeminformationen ermittelt werden. Dadurch lassen sich wiederum Kommunikationsschnittstellen ermitteln, sodass darauf aufbauend Angriffe geplant und durchgeführt werden. Auch Informationen zu Firmware etc. lassen sich für einen Angriff ermitteln und auswerten. Die Systeminformationen stellen daher selbst zunächst keine brisanten Informationen dar, sollten jedoch geschützt werden, um Planungen zukünftiger Angriffe zu erschweren.

***Beispiele:***

- Bei versiegelten Endgeräten wird das Siegel kopiert, um bei einer zukünftigen Hardwaremanipulation ein ähnliches Siegel anbringen zu können.
- Es wird das gerätespezifische Betriebssystem z.B. das Android Betriebssystem von Google© in der Version 4.2 festgestellt. Anschließend werden gezielt Sicherheitslücken für diese Version gesucht.

| Risiko | Gegenmaßnahme |
|---|---|
| **hoch** | Private Endgeräte dürfen nicht genutzt werden, da auf Nutzungsort, Aufbewahrungsort etc. kein Einfluss genommen werden kann. |
| **mittel** | Private Endgeräte werden versiegelt, sodass interne Hardwaremerkmale geschützt werden. Der Benutzer wird zusätzlich darüber aufgeklärt, dass Fremde das Telefon nicht benutzen sollen. |
| **gering** | Der Benutzer wird über die Gefahren informiert und darum gebeten, Fremden keinen Zugriff auf das dienstlich genutzte private Endgerät zu gewähren. |

### *R3 – Fremdnutzung*

Da nicht alle Endgeräte mandantenfähig sind, kann das Überlassen von Endgeräten an andere Personen, diesen Personen Zugang zu Informationen und Ressourcen des Unternehmens bieten. Dies kann besonders leicht geschehen, wenn Passwörter auf dem System gespeichert wurden.

***Beispiele:***

- Das Smartphone wird zum Telefonieren weitergegeben. Andere Person kann ggf. E-Mails oder SMS lesen und schreiben.
- Das Smartphone hat Zugangsdaten gespeichert, die exportiert werden können.

| Risiko | Gegenmaßnahme |
|---|---|
| **hoch** | Es dürfen keine privaten Endgeräte genutzt werden oder der Benutzer erklärt, dass notwendige Zugangskennungen lediglich ihm bekannt sind. Benutzerkennungen und Passwörter dürfen nicht gespeichert werden. Dienstliche Informationen müssen über entsprechende Passwörter geschützt werden. |
| **mittel** | Dienstliche Informationen dürfen nur nach Passworteingabe nutzbar werden. Passwörter dürfen nicht gespeichert werden. Ist das Endgerät mandantenfähig, können die Informationen direkt im gesicherten Profil gespeichert werden.g |
| **gering** | Das Endgerät muss über einen Zugriffsschutz (z.B. Passwort) verfügen und dienstliche Informationen mit einem Passwort versehen werden. |

### *R4 – Kopieren von Daten*

Wenn Angreifer sich im Besitz des mobilen Endgeräts befinden, so lassen sich Daten (ggf. durch Zerstörung des Endgeräts) über Schnittstellen oder Speicherkarten auslesen. Durch den Hardwarezugriff lassen sich je nach Architektur möglicherweise auch die kryptografischen Schlüssel auslesen, sodass verschlüsselte Inhalte entschlüsselt werden könnten.

***Beispiele:***

- Kopieren der unverschlüsselten Speicherkarte des mobilen Endgeräts durch Anschluss an einen Computer mittels Speicherkartenlesegerät
- Zugriff über Schnittstellen auf das mobile Endgerät

| Risiko | Gegenmaßnahme |
|---|---|
| **hoch** | Es dürfen nur Endgeräte verwendet werden, die eine dem Unternehmen entsprechende Verschlüsselung bieten. Ist dies nicht gegeben, dürfen die Daten nicht lokal gespeichert werden, sondern nur über eine verschlüsselte Netzwerkverbindung bei Bedarf geladen werden. Die Daten dürfen nach dem Aufruf nicht unverschlüsselt auf dem Endgerät verbleiben. |
| **mittel** | Es dürfen nur Endgeräte verwendet werden, die eine entsprechende Verschlüsselung bieten. Der Zugriff über verschlüsselte Netzwerkverbindungen ist erlaubt. |
| **gering** | Informationen auf extern auslesbarem Speicher (z.B. Speicherkarten) müssen verschlüsselt oder intern auf dem Endgerät gespeichert werden. |

### *R5 – Totalausfall*

Durch einem Ausfall der Hardware sind die bisher genutzten Dienste auf dem mobilen Endgerät zunächst nicht mehr verfügbar. Dabei spielt es keine Rolle, ob dieser Ausfall der Hardware technisch bedingt oder durch Manipulation erfolgt ist. Da meist ein Austausch oder eine Reparatur notwendig ist, verfügt die Person in dieser Zeit über kein Endgerät mehr. Bei privaten mobilen Endgeräten kann

die Reparaturdauer ein Vielfaches der Reparaturdauer eines dienstlich beschafften Endgerätes (ggf. mit Servicevertrag) betragen.

***Beispiele:***

- Das mobile Endgerät ist defekt und der Mitarbeiter aufgrund der Reparaturdauer länger nicht erreichbar.
- Der Mitarbeiter nutzt lediglich das private Notebook, welches auf einer Dienstreise einen Defekt erleidet. Die Reparatur möchte er jedoch erst zuhause durchführen lassen.

| Risiko | Gegenmaßnahme |
|---|---|
| **hoch** | Ist das Risiko so hoch, dass ein Ausfall nicht toleriert werden kann, muss die Versorgung durch dienstliche Endgeräte so sichergestellt werden, dass die Arbeit ohne das private Endgerät ebenfalls möglich ist. |
| **mittel** | Im Falle von Ausfällen müssen dienstliche Endgeräte zeitweise zur Verfügung gestellt werden können oder die Aufgaben auf anderem Wege erfolgen können. |
| **gering** | Entfällt, da eine zeitnahe Reaktion nicht erforderlich sein sollte. |

### *R6 – offene Sicherheitslücken*

Werden Endgeräte mit eigenem Betriebssystem nicht durch Patches aktualisiert, so können bekannte Sicherheitslücken dazu führen, gespeicherte Informationen der Endgeräte auszulesen. Beim Einsatz von mobilen Endgeräten werden im privaten Umfeld teilweise auch Betriebssystemvarianten die nicht vom Hersteller stammen installiert oder sogenannte Jailbreaks durchgeführt. Dies ermöglicht dem Endnutzer höhere Freiheitsgrade, sodass vom Hersteller nicht vorgesehene Funktionen (Rootzugriff, kostenfreie Installation urheberrechtlich geschützter Anwendungen, etc.) möglich werden. Von Nachteil ist jedoch, dass nach diesen Aktionen meist keine Updates der Hersteller mehr eingespielt werden können, sodass Sicherheitslücken nicht geschlossen werden.

***Beispiele:***

- Durch Sicherheitslücken können Angreifer Administratorrechte auf dem System erlangen und beliebige weitere Software auf das Gerät aufspielen und ausführen.
- Durch Fehler im Betriebssystem kann das System (meist vorübergehend) zum Ausfall gebracht werden, sodass es für die benötigten Aufgaben nicht weiter zur Verfügung steht.

| Risiko | Gegenmaßnahme |
|---|---|
| **hoch** | Es dürfen nur Endgeräte eingesetzt werden, die mit einem Agenten versehen sind, der den aktuellen Systemzustand verifiziert und Rückmeldungen an die IT-Abteilung des Unternehmens liefern kann. Es dürfen nur vom Hersteller zur Verfügung gestellte Betriebssysteme verwendet werden. Zusätzliche Sicherheitssoftware (z.B. ein Virenscanner - je nach Unternehmensstandard) muss genutzt werden. |
| **mittel** | Es dürfen nur Endgeräte eingesetzt werden, die ein vom Hersteller zugelassenes Betriebssystem verwenden. Der Benutzer hat sicherzustellen, dass die möglichen Sicherheitsfunktionen genutzt werden und Updates zeitnah implementiert werden. |
| **gering** | Es dürfen nur Endgeräte eingesetzt werden, die ein vom Hersteller zugelassenes Betriebssystem verwenden |

### *R7 – Schaden durch Software*

Ebenso wie im Betriebssystem können sich Sicherheitslücken auch in Anwendungen befinden. Diese können meist ebenfalls durch einen Patch behoben werden. So kann die Wahrscheinlichkeit eines Sicherheitsvorfalls gesenkt werden. Werden jedoch im Fall von privaten Endgeräten neben den notwendigen geschäftlichen Anwendungen weitere Anwendungen installiert, die nicht auf

Sicherheitsrisiken überprüft wurden, so kann durch diese Anwendungen ein erhöhtes Risiko entstehen. Neben tatsächlichen Sicherheitslücken sind auch die Funktionen der Anwendungen selbst zu überdenken. So sammeln manche Anwendungen Informationen auf den Endgeräten und übertragen diese an Dritte.

***Beispiele:***

- Eine Anwendung sendet das Adressbuch des Unternehmens an einen Dritten, der die Daten für bspw. Werbemaßnahmen nutzt.
- Ein Programm zur Dateisynchronisation sendet Unternehmensdaten aufgrund falscher Konfiguration von einem privaten PC an Dritte.

| Risiko | Gegenmaßnahme |
|---|---|
| **hoch** | Um unerwünschte Einwirkungen von Anwendungen ausschließen zu können, dürfen ausschließlich die auf einer Positiv-Liste geführten Anwendungen installiert und genutzt werden. |
| **mittel** | Anwendungen, die nicht auf einer Negativ-Liste genannt werden, dürfen nicht installiert werden. Bei nicht genannten Programmen müssen vor einer Installation die Angaben des Herstellers in Bezug auf die System- und Informationssicherheit geprüft werden. Dabei ist sicherzustellen, dass Dritte keine Informationen erlangen oder manipulieren können. |
| **gering** | Anwendungen oder Anwendungen mit bestimmten Merkmalen, die nicht explizit auf einer Negativ-Liste geführt werden, dürfen installiert und genutzt werden. |

### *R8 – einfache Passwörter*

Werden auf privaten Endgeräten einfache Passwörter (z.B. Passwörter ohne Zahlenkombinationen oder Sonderzeichen) verwendet, so sind diese durch verschiedene Techniken wie Raten oder spezifischen Angriffen (z.B. BruteForce) leicht zu ermitteln. Da im privaten Umfeld keine Passwortrichtlinien durchgesetzt werden können, kann es sogar vorkommen, dass Endgeräte über keinen Zugangsschutz verfügen.

***Beispiele:***

- Das Passwort ist der Name der Freundin des Besitzers des Endgeräts.
- Das Passwort ist nicht vorhanden, man muss lediglich die „Tastensperre“ des mobilen Endgeräts lösen.

| Risiko | Gegenmaßnahme |
|---|---|
| **hoch** | Es dürfen ausschließlich Endgeräte verwendet werden, die zur Nutzung eine Authentifizierung verlangen, die mindestens den Standards des Unternehmens entspricht. |
| **mittel** | Es müssen Vorkehrungen getroffen werden, um die Funktionen vor Fremden mit kurzfristigen Endgerätezugriff zu schützen. Dies kann etwa durch die Eingabe eines Pins erfolgen. |
| **gering** | Es müssen Vorkehrungen getroffen werden, um die Funktionen vor unbeabsichtigtem Zugriff (z.B. spielende Kinder) zu schützen. |

### *R9 – Denial of Service (DoS)*

Bietet ein Betriebssystem Dienste über Schnittstellen an, so kann durch ein Überlasten dieses Dienstes, der Dienst für den Nutzer gestört werden. Der Angreifer erzeugt dabei eine ausreichend hohe Anzahl an Anfragen, sodass der Dienst keine Ressourcen für weitere Anfragen nutzen kann.

***Beispiele:***

- Permanente Anrufe über einen längeren Zeitraum auf einem mobiles Endgerät mit Telefonfunktion
- Belegung der Bandbreite eines Netzzugangs, sodass Netzwerkverbindungen nicht oder nur sehr langsam aufgebaut werden können.

| Risiko | Gegenmaßnahme |
|---|---|
| **hoch** | Um Endgeräte vor DoS-Angriffen zu schützen, muss die Kommunikation durch Software oder Hardware zu unterbrechen sein. Gleichzeitig muss die Möglichkeit bestehen, über andere Wege die Aufgaben bearbeiten zu können. |
| **mittel** | Es sind keine Maßnahmen erforderlich. |
| **gering** | Es sind keine Maßnahmen erforderlich. |

### *R10 – keine Updates*

Werden vorgesehene Updates nicht zeitnah installiert, so können Angriffe auf bereits öffentlich bekannte Sicherheitslücken durchgeführt werden. Da besonders bei privaten Endgeräten eine Verifizierung der Updates in der Verantwortung des Nutzers liegt, kann das Unternehmen nicht sicherstellen, dass alle relevanten Updates installiert sind. Somit sind diese Endgeräte einer erhöhten Gefahr ausgesetzt.

***Beispiele:***

- Der Benutzer des mobilen Endgeräts installiert keine Updates.
- Durch den Jailbreak eines Apple-Gerätes können keine neuen Updates des Herstellers installiert werden.

| Risiko | Gegenmaßnahme |
|---|---|
| **hoch** | Updates müssen innerhalb einer vorgegebenen Frist installiert werden. Zur Verifizierung können stichpunktartige Kontrollen vorgenommen werden. Bei bekannten Sicherheitslücken, für die kein Update bereitgestellt wurde, darf das Endgerät nicht weiter verwendet werden. |
| **mittel** | Updates müssen innerhalb einer vorgegebenen Frist installiert werden. Überprüfungen finden im Verdachtsfall statt. |
| **gering** | Updates müssen innerhalb einer vorgegebenen Frist installiert werden. Eine Überprüfung findet nicht statt. |

### *R11 – Vermischung von Daten*

Falls Endgeräte die Synchronisierung oder Speicherung von Daten unterstützen, kann es besonders bei privat genutzten Endgeräten dazu führen, dass private und geschäftliche Daten vermischt werden. Dies bedeutet, dass geschäftliche Daten ggf. im Rahmen der Weitergabe privater Daten ebenfalls weitergegeben werden oder dass private Daten auf Ressourcen im Unternehmen gespeichert werden und dort Ressourcen belegen.

***Beispiele:***

- Die Synchronisation des Adressbuchs mit den Rechnern des Unternehmens kann dazu führen, dass auch private Kontakte im Unternehmen gespeichert werden.
- Bei der gemischten Verwendung eines Speichergeräts kann der Benutzer die geschäftlichen Daten "vergessen", sodass bei einem privaten Datenaustausch fremde Personen ebenfalls Zugriff auf die geschäftlichen Informationen erhalten.

| Risiko | Gegenmaßnahme |
|---|---|
| **hoch** | Es dürfen ausschließlich mandantenfähige Endgeräte verwendet werden, die eine strikte Trennung dienstlicher und privater Daten ermöglichen. Eine Vermischung in beide Richtungen ist auszuschließen. |
| **mittel** | Die Trennung privater und dienstlicher Daten kann auf der Anwendungsebene erfolgen. Dienstliche Daten dürfen dabei nicht in den Bereich der privaten gelangen können. |
| **gering** | Die Trennung privater und dienstlicher Daten sollte gekennzeichnet sein, sodass eine Bereinigung möglich ist. |

### *R12 – Konfigurationsänderung*

Durch Konfigurationsänderungen am Betriebssystem lassen sich verschiedene Auswirkungen erzielen. Diese reichen von der völligen Unbrauchbarkeit des Endgerätes bis hin zur Manipulation von Kommunikationswegen.

***Beispiele:***

- An einem Endgerät wird die Sprache umgestellt, sodass ein Nutzer das Menü nicht mehr verwenden kann.
- Es wird die automatische Verwendung eines sog. Proxyserver eingestellt, sodass sämtlicher unverschlüsselter Datenverkehr mitgelesen werden kann. Besonders diese Einstellung wird dem normalen Nutzer kaum auffallen, da er das Endgerät wie gewohnt nutzen kann.

| Risiko | Gegenmaßnahme |
|---|---|
| **hoch** | Konfigurationen dürfen nur nach Eingabe eines Passwortes, welches sich vom "Entsperrcode" des Endgeräts unterscheidet, möglich sein. Die Einstellungen müssen von der IT des Unternehmens jederzeit prüfbar und veränderbar sein. |
| **mittel** | Konfigurationen dürfen nur nach Eingabe eines Passwortes, welches sich vom "Entsperrcode" des Endgeräts unterscheidet, möglich sein. Von Vorgaben des Unternehmens darf nicht abgewichen werden. |
| **gering** | Konfigurationen dürfen nur nach Eingabe eines Passwortes möglich sein. Von Vorgaben des Unternehmens darf nicht abgewichen werden. |

### *R13 – Unerwünschte Sensornutzung*

Da das Betriebssystem auch den Zugriff auf Sensoren der Endgeräte steuert, ist es ebenfalls möglich, Sensoren zu missbrauchen. Sensoren könnten Daten zu bestimmten Zeiten erfassen und speichern und sofort oder zeitverzögert an einen Rechner des Angreifers übertragen.

***Beispiele:***

- Ein Mikrofon, welches in das Endgerät eingebaut wurde, schneidet Gespräche mit, die anschließend über eine Internetverbindung verschickt werden.
- Gleiches wäre auch mit Sensoren wie Kamera (Bilder) oder GPS (Positionsdaten, Wegstrecken) möglich.

| Risiko | Gegenmaßnahme |
|---|---|
| **hoch** | Sensoren müssen in einer Form deaktiviert werden, dass ihre Nutzung ausgeschlossen ist und dieser Zustand verifizierbar ist. Vom Unternehmen ausgegebene Siegel, die die Linse einer Kamera überdecken, erfüllen diesen Zweck. Ist dies nicht sicherzustellen, dürfen die Endgeräte nicht verwendet werden. |
| **mittel** | Sensoren müssen durch Softwarefunktionen deaktivierbar sein. Dies muss durch die IT-Abteilung des Unternehmens verifizierbar sein. Ist dies nicht möglich, dürfen diese Endgeräte nur außerhalb bestimmter Bereiche verwendet werden. |
| **gering** | Sensoren müssen durch Softwarefunktionen deaktivierbar sein. Die Deaktivierung und Aktivierung kann durch den Nutzer selbst erfolgen. |

### *R14 – Verbreitung von Schadsoftware*

Infizierte Systeme, die bereits legalen Zugriff auf Infrastrukturen besitzen, können leichter weitere Systeme infizieren, da sie zunächst als vertrauenswürdig identifiziert werden. Dies kann dazu führen, dass sich die Schadsoftware – z.B. ein Virus – auf nicht ausreichend geschützte Computersysteme von Kollegen des Nutzers des Endgeräts überträgt.

***Beispiele:***

- Ein Computer mit Virus wählt sich per sicherer Netzwerkverbindung (z.B. einer VPN-Verbindung) in das Unternehmensnetzwerk ein und der Virus attackiert ein nicht geschütztes System, welches aus dem Internet sonst nicht erreichbar wäre.
- Ein befallener Computer sendet den Virus über die Infrastruktur per Email an Kollegen, die mögliche Anhänge als sicher einstufen und sich somit ebenfalls identifizieren.

| Risiko | Gegenmaßnahme |
|---|---|
| **hoch** | Es dürfen nur Endgeräte, die die *hohen* Gegenmaßnahmen gegen<br>– R6 (Ausnutzen von Sicherheitslücken)<br>– R7 (Schaden durch Software)<br>– R10 (Nicht vorhandene Updates)<br>– R14 (Verbreitung von Schadsoftware)<br>umsetzen, eine direkte Verbindung zu internen IT-Systemen aufbauen. |
| **mittel** | Es dürfen nur Endgeräte, die die *mittleren* Gegenmaßnahmen gegen<br>– R6 (Ausnutzen von Sicherheitslücken)<br>– R7 (Schaden durch Software)<br>– R10 (Nicht vorhandene Updates)<br>– R14 (Verbreitung von Schadsoftware)<br>umsetzen, eine direkte Verbindung zu internen IT-Systemen aufbauen. |
| **gering** | Es dürfen nur Endgeräte, die die *geringen* Gegenmaßnahmen gegen<br>– R6 (Ausnutzen von Sicherheitslücken)<br>– R7 (Schaden durch Software)<br>– R10 (Nicht vorhandene Updates)<br>– R14 (Verbreitung von Schadsoftware)<br>umsetzen, eine direkte Verbindung zu internen IT-Systemen aufbauen. |

### *R15 – Unautorisierte Verwendung*

Infrastrukturen bieten eine große Anzahl an Informationen und Diensten. Wird ein Endgerät mit Zugriff auf diese Infrastrukturen unerlaubterweise verwendet, kann es dazu führen, dass nicht

berechtigte Personen Zugriff auf diese Dienste und Informationen erhalten. Dies kann besonders dann geschehen, wenn Zugangspasswörter auf den Endgeräten gespeichert wurden.

***Beispiele:***

- Fremde benutzen einen Laptop mit einer sicheren Netzwerkverbindung und einem gespeichertem Passwort, um Informationen aus dem internen Portal des Unternehmens zu sammeln.
- Ein Computerwurm benutzt Server des Unternehmens unauffällig zur Kommunikation mit anderen befallenen Computern (z.B. Steuerung eines Bot-Netzwerkes).

| Risiko | Gegenmaßnahme |
|---|---|
| **hoch** | Zugriffe auf die IT-Systeme dürfen nur nach Eingabe eines Einmal-Passwortes erfolgen. Die Generierungsregeln des Einmal-Passwortes dürfen nur dem Berechtigten bekannt sein und müssen sich aus Besitzinformationen und Wissensinformationen zusammensetzen. |
| **mittel** | Zugriffe auf die IT-Systeme dürfen nur nach Eingabe eines Passwortes erfolgen, welches nicht auf dem Endgerät gespeichert werden kann. |
| **gering** | Zugriffe auf die IT-Systeme dürfen nur nach Eingabe eines Passwortes erfolgen. |

### *R16 – DoS gegen Infrastruktur*

Endgeräte können durch Fehlkonfigurationen oder aufgrund eines Virusbefalls DoS-Attacken gegen Infrastrukturen beginnen. Der wiederholte Zugriff (oder Versuch eines Zugriffs) auf Ressourcen kann dazu führen, dass andere berechtigte Nutzer den Dienst aufgrund einer Überlastung nicht mehr nutzen können.

***Beispiele:***

- Oftmals werden Accounts nach einer bestimmten Anzahl falsch eingegebener Passwörter – zumindest für eine spezifische Zeitspanne – gesperrt. Ein Angriffsszenario könnte somit sein, Versuche des Einwählens mit fremden Accounts so oft durchzuführen, dass diese aus Sicherheitsgründen gesperrt werden. Aufgrund der Sperrung können jedoch die berechtigten Benutzer auch mit dem richtigen Passwort keine Anmeldungen mehr vornehmen, sodass diese keine Dienste mehr nutzen können.
- Werden E-Mails an Benutzer versendet, die keine für den Benutzer relevanten Informationen oder sogar Werbung enthalten und den Benutzer stören (SPAM), werden diese E-Mails meistens bereits von einem zentralen System herausgefiltert. Werden diese jedoch von einem vertrauenswürdigen Account innerhalb des Unternehmens versendet, werden die E-Mails in der Regel zugestellt. So können Mitarbeiter mit E-Mail überflutet werden, sodass die notwendigen E-Mails nicht mehr abgearbeitet werden können.

| Risiko | Gegenmaßnahme |
|---|---|
| **hoch** | Durch vorgegebene Konfigurationen der dienstlich genutzten Komponenten soll sichergestellt werden, dass durch Fehlkonfigurationen Dienste zu stark belastet werden. |
| **mittel** | Durch vorgegebene Konfigurationen der dienstlich genutzten Komponenten soll sichergestellt werden, dass durch Fehlkonfigurationen Dienste zu stark belastet werden. |
| **gering** | Durch vorgegebene Konfigurationen der dienstlich genutzten Komponenten soll sichergestellt werden, dass durch Fehlkonfigurationen Dienste zu stark belastet werden. |

### *R17 – Ermittlung von Gegenmaßnahmen*

Es existieren häufig Vorgehensmodelle im Angriffsfall, die ein systematisches Verhindern von Störungen ermöglichen sollen. Angreifer sollen durch dieses Vorgehen daran gehindert werden, Informationen auszulesen oder Infrastrukturen zu stören. Aus Sicht der Angreifer sind besonders die geplanten und möglichen Gegenmaßnahmen von Interesse, da die Angreifer sich darauf vorbereiten können. Daher ist das Ermitteln von Gegenmaßnahmen meist nur eine Vorbereitungsmaßnahme eines folgenden Angriffs.

***Beispiele:***

- Ermitteln von Reaktionszeiten, die vorgesehen sind, um Accounts zu sperren oder E-Mail-Absender zu blockieren.
- Ermitteln von Lastgrenzen, die als Indikator für Sicherheitssysteme dienen, das angreifende System zu sperren. So kann beispielsweise ermittelt werden, wie viele Systeme mit welcher individuellen Last zusammen wirken können, sodass das System gestört wird, jedoch kein Angriffssystem geblockt wird.

| Risiko | Gegenmaßnahme |
|---|---|
| **hoch** | Endgeräte, die dazu genutzt werden können, Gegenmaßnahmen der Infrastruktur im Angriffsfall auszuspähen, müssen gegen den Zugriff Unberechtigter geschützt werden. Nach einer bestimmten Anzahl fehlerhafter Zugriffsversuche muss das Endgerät die Konfiguration selbstständig entfernen, sodass keine weiteren Zugriffsversuche unternommen werden können. |
| **mittel** | Endgeräte sind vor der Nutzung durch Unberechtigte zu schützen. Dazu zählen auch die Gegenmaßnahmen zu R2. |
| **gering** | Es sind keine Maßnahmen erforderlich. |

### *R18 – Bluetooth-spezifisch*

Bluetooth wird oftmals zur Kommunikation zwischen Endgeräten wie Smartphones und Laptops eingesetzt. Drahtlose Headsets bedienen sich meist ebenfalls der Bluetooth Technologie. Neben der reinen Störung der Verbindung kann auch ein Abhören und Manipulieren der übertragenen Daten in Frage kommen. Möglicherweise können auch Steuerungssignale an ein Endgerät gesendet werden.

***Beispiele:***

- Der Bluetooth Verbindungsaufbau wird gestört, sodass dieser erneut aufgebaut werden muss, wobei der Angreifer die eingesetzten Schlüssel erhalten kann und somit die weitere Kommunikation mitlesen kann.
- Bluetooth Endgeräte werden „versehentlich“ gepaart (z.B. Verbindungen mit einem Endgerät gleichen Namens, sodass der Endanwender die Endgeräte nicht leicht unterscheiden kann) und bieten anschließend Funktionen, die das Auslesen von Daten ermöglichen.

| Risiko | Gegenmaßnahme |
|---|---|
| **hoch** | Bluetooth darf nicht genutzt werden und darf nicht eingeschaltet sein. |
| **mittel** | Bluetooth darf nur im Modus 3 eingesetzt werden. Dies erfordert eine Authentifizierung sowie zusätzlich eine Verschlüsselung der übertragenen Daten. |
| **gering** | Bluetooth darf uneingeschränkt genutzt werden. Die Sichtbarkeit der Endgeräte ist auf notwendige Zeiträume zu beschränken. |

### *R19 – Infrarotschnittstellen-spezifisch*

Da die Infrarotschnittstelle (IrDA-Schnittstelle) über Lichtwellen kommuniziert, sind diese im Umfeld ebenfalls von anderen Geräten zu empfangen. Aufgrund der geringen Leistung ist dies jedoch nur im direkten Umfeld des sendenden Endgerätes möglich. Weiterhin ist zu beachten, dass die IrDA-Schnittstelle keine Authentifikation erfordert, sodass gesendete Daten sofort angenommen werden.

***Beispiele:***

- Daten werden von einem Angreifer gesendet und die aktivierte Schnittstelle führt aufgrund einer Sicherheitslücke die Befehle ungefragt aus.
- Daten werden übertragen und gleichzeitig von einem Angreifer mitgelesen.

| Risiko | Gegenmaßnahme |
|---|---|
| **Hoch** | Die Infrarotschnittstelle ist zu deaktivieren und mit einer Abdeckung (Siegel) zu versehen, sodass die Nutzung ausgeschlossen ist. |
| **Mittel** | Die Infrarotschnittstelle ist zu deaktivieren und darf für die Übertragung dienstlicher Informationen nicht genutzt werden. |
| **Gering** | Die Infrarotschnittstelle ist nur in geschlossenen Räumen und unter Abwesenheit Unbefugter zu nutzen, wenn kein sichererer Übertragungsweg möglich ist. |

### *R20 – WLAN-spezifisch*

Die WLAN-Schnittstelle bietet verschiedene Kommunikationsmöglichkeiten an. So ist die Nutzung eines Accesspoints möglich, bei der das Endgerät als Nutzer der Infrastruktur auftritt und verfügbare Angebote annimmt. Ebenfalls existiert meist die Option, selbst als Infrastrukturanbieter zu fungieren und einen Accesspoint bereitzustellen. Im Fall, dass ein mobiles Endgerät als Accesspoint angeboten wird, kann bei unzureichendem Schutz möglicherweise nicht verhindert werden, dass Fremde den Zugang ebenfalls nutzen und ggf. auch Zugang zu internen Infrastrukturen erhalten.

***Beispiele:***

- Der Angreifer bietet einen kostenlosen WLAN-Zugang und liest die übertragenen Daten mit.
- Der Angreifer nutzt die eingeschaltete Funktion eines Accesspoint eines Smartphones, um auf das interne Firmennetzwerk zuzugreifen.

| Risiko | Gegenmaßnahme |
|---|---|
| **hoch** | Die WLAN-Schnittstelle darf ausschließlich zur Verbindung mit bekannten und per Zertifikat signierten Accesspoints genutzt werden. Dabei darf ausschließlich WPA2 zum Einsatz kommen. |
| **mittel** | Die WLAN-Schnittstelle darf ausschließlich zur Verbindung mit bekannten Accesspoints genutzt werden. Dabei darf ausschließlich WPA2 zum Einsatz kommen. |
| **gering** | Die WLAN-Schnittstelle darf zur Verbindung mit bekannten Accesspoints genutzt werden. Dabei darf ausschließlich WPA2 zum Einsatz kommen. Eigene Hotspots dürfen mit dem Endgerät lediglich kurzzeitig erstellt werden, wenn keine andere Möglichkeit besteht. Dabei muss ebenfalls WPA2 verwendet werden. Die Schlüssellänge und Komplexität wird von der IT-Abteilung des Unternehmens festgelegt. |

### *R21 – NFC-spezifisch*

NFC bietet eine Kommunikationsmöglichkeit über sehr kurze Distanzen. Hat der Angreifer Zugriff auf das Endgerät, oder kann sich ihm unauffällig nähern, so kann bereits die NFC-Kommunikation genutzt werden. Je nach Konfiguration des Endgerätes kann dies dazu führen, dass Aktionen durchgeführt werden, durch die ein Schaden entstehen kann.

***Beispiele:***

- Der Angreifer ändert die Konfiguration des Endgeräts derart, dass ihm weitere Angriffe möglich sind.
- Der Angreifer führt als Aktion die Wahl einer kostenpflichtigen Rufnummer durch.

| Risiko | Gegenmaßnahme |
|---|---|
| **hoch** | Die NFC-Kommunikationsschnittstelle permanent abgeschaltet werden und darf nicht genutzt werden. |
| **mittel** | Die NFC-Kommunikationsschnittstelle darf nur durch manuelle Aktivierung des Benutzers für einen begrenzten Zeitraum aktiviert werden. |
| **gering** | Es sind keine Maßnahmen erforderlich. |

### *R22 – Kommunikationsangriffe*

Bei der Nutzung von Kommunikationsschnittstellen ist es notwendig, sicherzustellen, dass der Kommunikationspartner der gewünschte ist und die Informationen auf direktem Weg erhält. Ein möglicher "Man-In-The-Middle" könnte beispielsweise als Relaystation zwischen den Kommunikationspartnern stehen und die Kommunikation weiterleiten, sodass die Kommunikation weiterhin erfolgreich ist.

***Beispiele:***

- Wie bereits im Beispiel WLAN beschrieben, kann ein Angreifer einen WLAN-Accesspoint simulieren und die versendeten Daten mitlesen. Wird keine Verschlüsselung eingesetzt, kann in Echtzeit der Klartext mitgelesen und ausgewertet werden.
- In der gleichen Situation wie im ersten Beispiel, wäre es dem Angreifer ebenfalls möglich, die übertragenen Informationen zu verändern. So kann beispielsweise eine Telefonnummer zur Kontaktaufnahme von einer Website durch die des Angreifers ausgetauscht werden, sodass der Nutzer auch bei einer telefonischen Kontaktaufnahme den Angreifer erreicht[1]

| Risiko | Gegenmaßnahme |
|---|---|
| **hoch** | Zu schützende Informationen dürfen ausschließlich verschlüsselt übertragen werden (z.B. via VPN oder HTTPS). Die Systeme müssen dabei über Zertifikate verfügen, die neben der Verschlüsselung einen verifizierbaren Identitätsnachweis erbringen können. Auf den Endgeräten dürfen nur Verbindungen zu vertrauenswürdigen Systemen aufgebaut werden, die durch ein Zertifikat verifiziert wurden. Es sind ausschließlich vom Unternehmen freigegebene Wurzelzertifikate zu verwenden. |
| **mittel** | Zu schützende Informationen dürfen ausschließlich verschlüsselt übertragen werden (z.B. via VPN oder HTTPS). Die Systeme müssen dabei über Zertifikate verfügen, die neben der Verschlüsselung einen Identitätsnachweis erbringen können. Auf den Endgeräten dürfen nur Verbindungen zu vertrauenswürdigen Systemen aufgebaut werden. |
| **gering** | Zu schützende Informationen dürfen ausschließlich verschlüsselt übertragen werden (z.B. via VPN oder HTTPS). Auf den Endgeräten dürfen nur Verbindungen zu vertrauenswürdigen Systemen aufgebaut werden. |

## Zusammenfassung

Die hier vorgestellten Gegenmaßnahmen wurden im Projekt je nach Risiko, Eintrittswahrscheinlichkeit und potentieller Auswirkung den einzelnen im Unternehmen existierenden Risiken und deren

[1] Dieser könnte das Gespräch ebenfalls entgegennehmen oder weiterleiten und mithören

Ausprägung zugeordnet. Im Rahmen der Richtlinienentwicklung zur Umsetzung der BYOD-Strategie im Unternehmen wurde durch diese Zuordnungen auch die Sicherstellung der Informationssicherheit unterstützt. Durch die einfache Zuordnung waren die Risiken sowie die notwendigen Gegenmaßnahmen leicht individualisieren und konnte auf weitere Gerätegenerationen (z.B. eingestellter Auszubildender im Unternehmen) angewandt werden.

## Literatur

[1] Bundesamt für Sicherheit in der Informationstechnik (2008): Mobile Endgeräte und mobile Applikationen: Sicherheitsgefährdungen und Schutzmaßnahmen. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/MobilEndgeraete/mobile_endgeraete_pdf.pdf?__blob=publicationFile. Abgerufen am 30.08.2013