cogitron
Verstand für Systeme

Dr. H. Herrmann
MSc. M. Huber
Dr. H. Putzer

(v1.0) 22. Oktober 2020

"A Way into Your Heart"

Reife (-Grade) für Medizin-Cybersecurity: Darstellung an einem praktischen Beispiel

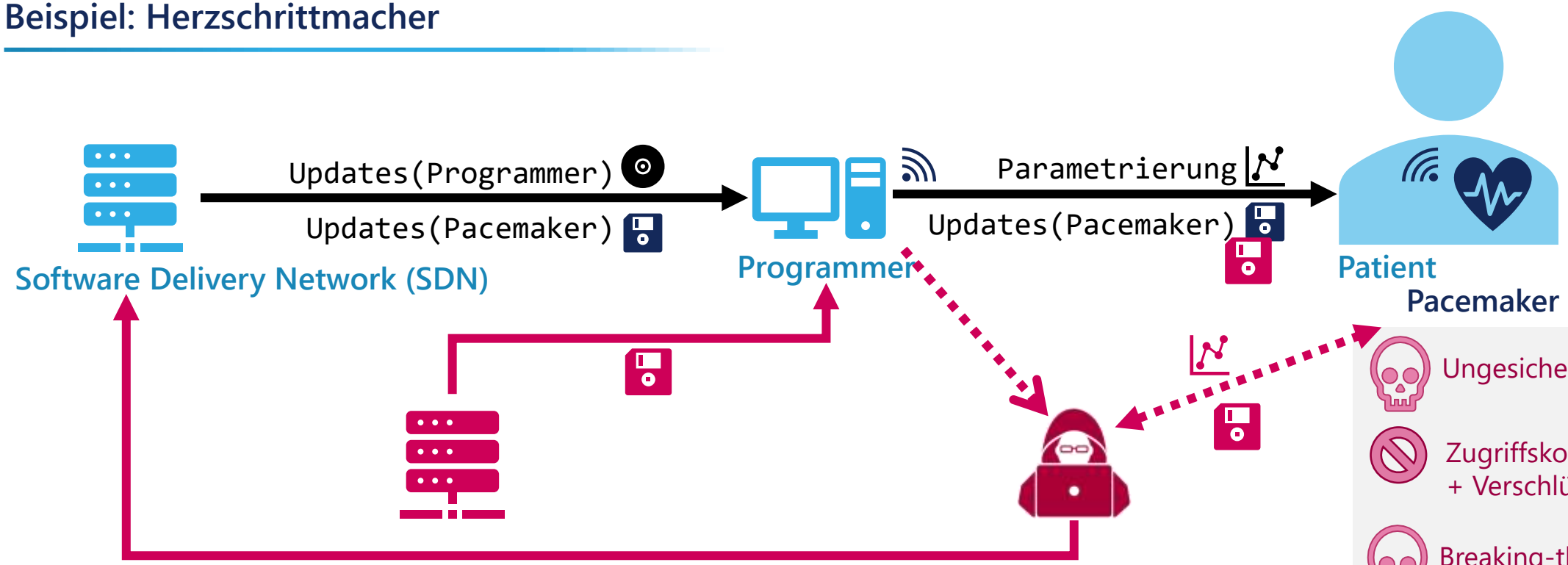
Motivation

Bildquelle: iStock Photo

- Uns umgeben IoT-Geräte mit komplexen Schnittstellen.
- Können wir diesen Schnittstellen vertrauen?
- Auch Medizingeräte sind betroffen.
- Es gibt Fälle, welche das Ziel „safe & effective“ verletzen (z.B. [1] & [2]).

Ref:
[1] Fabian A. Scherschel: “Möchten Sie sterben? Malware gegen Herzschrittmacher lässt Hersteller kalt“, HEISE, https://www.heise.de/security/meldung/Moechten-Sie-sterben-Malware-gegen-Herzschrittmacher-laesst-Hersteller-kalt-4133625.html
[2] Kerkmann, Nagel: „Todesfall nach Hackerangriff auf Uni-Klinik Düsseldorf “, HANDELSBLATT, https://www.handelsblatt.com/technik/sicherheit-im-netz/cyberkriminalitaet-todesfall-nach-hackerangriff-auf-uni-klinik-duesseldorf/v_detail_tab_print/26198688.html

Beispiel: Herzschrittmacher

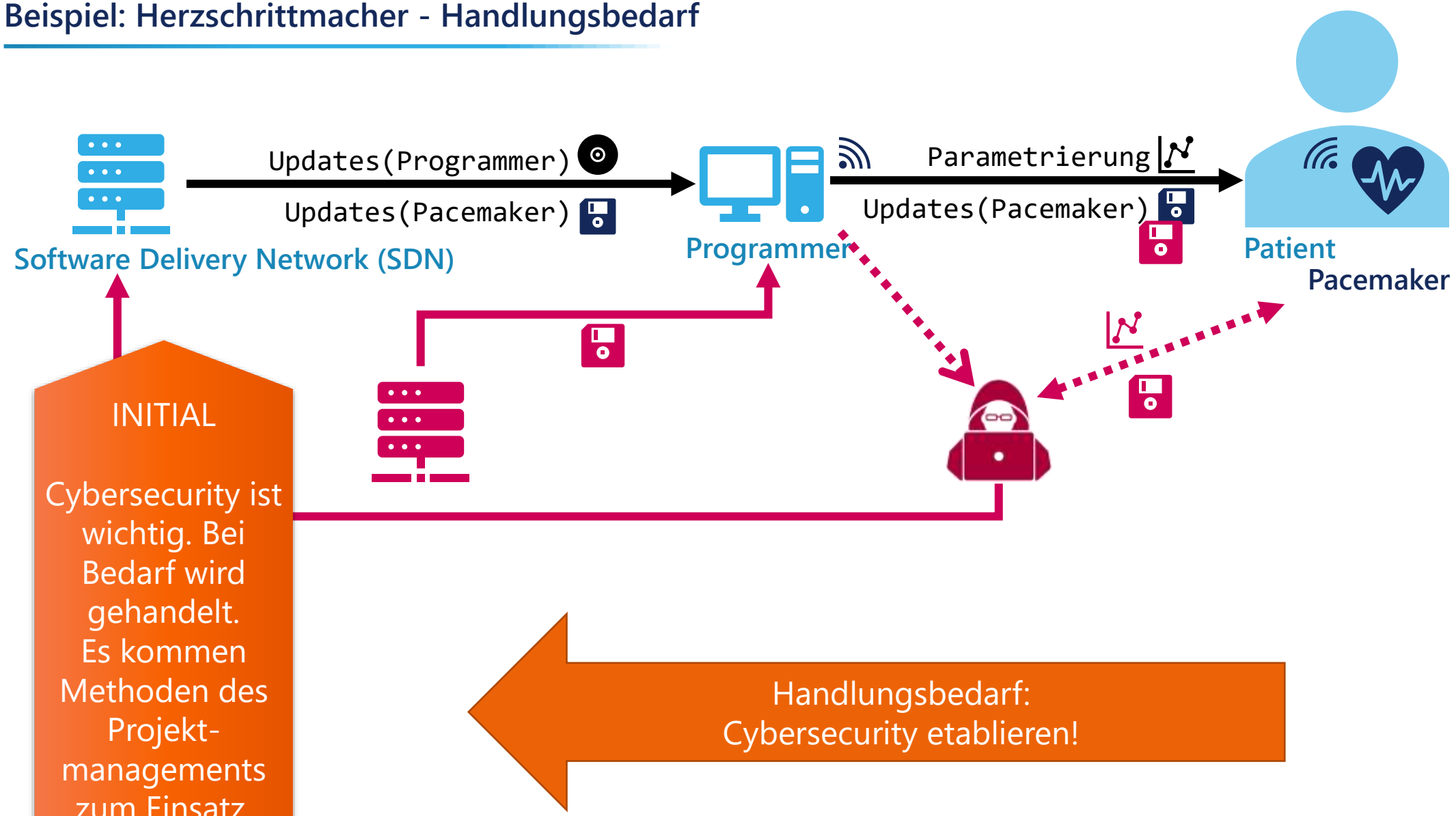


- Herzschrittmacher als lebenswichtiges Medizingerät
- Herzschrittmacher hat notwendige Schnittstellen (Parameter, Firmware)
- Herzschrittmacher wird angreifbar.
- Reicht das Ping-Pong zwischen Angreifer und Hersteller?

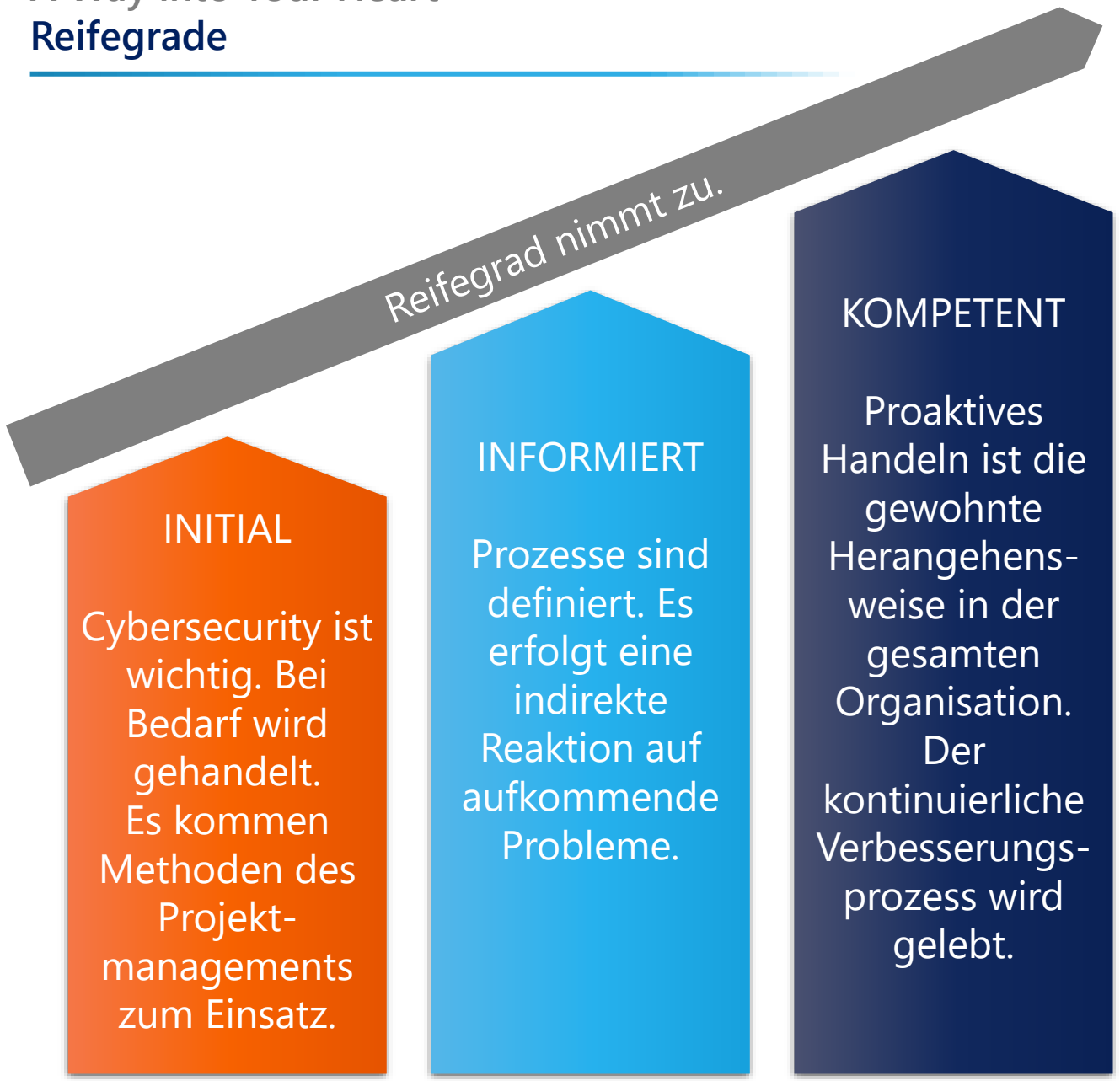
➢ Cybersecurity des Herstellers lebenswichtig für Patient!

- Ungesicherter Kanal
- Zugriffskontrolle + Verschlüsselung
- Breaking-the-Glass Policy
- Rechtemanagement
- Back End
- <weitere Gegenmaßnahmen>
- <weitere Schwachstellen>

Beispiel: Herzschrittmacher - Handlungsbedarf



Reifegrade



- **Initial**
  - Die Notwendigkeit zum Handeln ist erkannt. Tritt der Bedarf auf, wird zur Tat geschritten.
- **Informiert**
  - Grundsätzlich ist der Cybersecurity-Prozess definiert. Die Risiken werden analysiert und bewertet. Maßnahmen zur Risikominderung werden betrieben. Es gibt ein System zur Verfolgung und Erfassung von Security-Vorfällen und/oder der Veröffentlichung von Schwachstellen.
- **Kompetent**
  - Jeder in der Organisation weiß, was zu tun ist, wenn ein Vorfall auftritt (Cybersecurity Kultur). Prozesse sind messbar – Aufwände und Kosten sind transparent. Der kontinuierliche Verbesserungsprozess (KVP) wird gelebt.

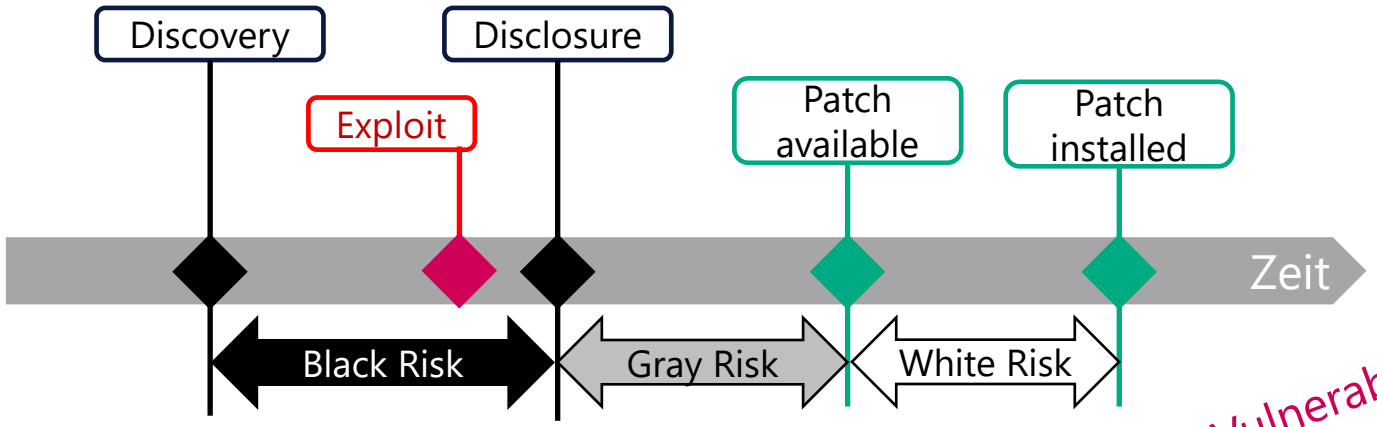
Reifegrad INITIAL

- **Die Notwendigkeit zum Handeln ist erkannt.**
- **Tritt der Bedarf auf, wird zur Tat geschritten.**
- **Quartalsweise Prüfung der Warn- und Informationsdienste.**
- **Risiken, die man nicht kennt, kann man auch nicht verwalten.**
- **Projekt oder Task Force:**
  - Plan
  - Mannschaft allokiert
  - Fachleute suchen (Beispielweise wenn kein PEN-Tester im Haus)
  - Ausführung, etc.
- **Konformität gegeben: z.B. MDR Artikel 87 (Vigilanz)**

Reifegrad INITIAL

- **Beispiel – Incident-Management**
  - Nur sporadisches Prüfen von Warn- und Informationsdiensten
  - Weitgehend Reaktiv

- **Ping-Pong zwischen Angreifern und Hersteller kostspielig**

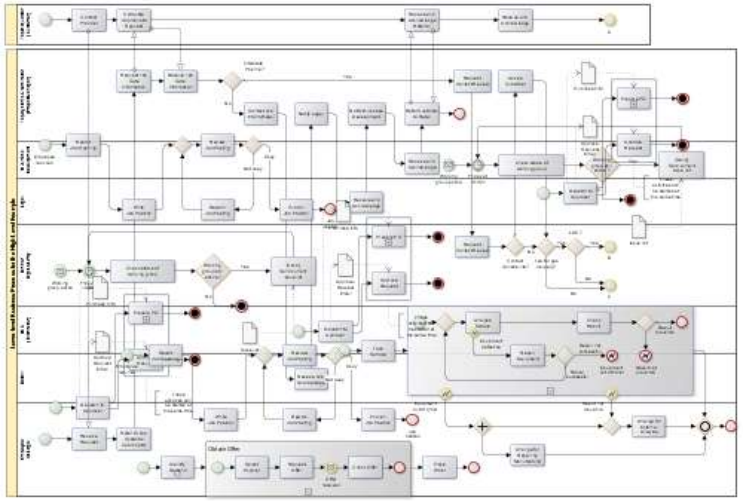


Vulnerability Lifecycle

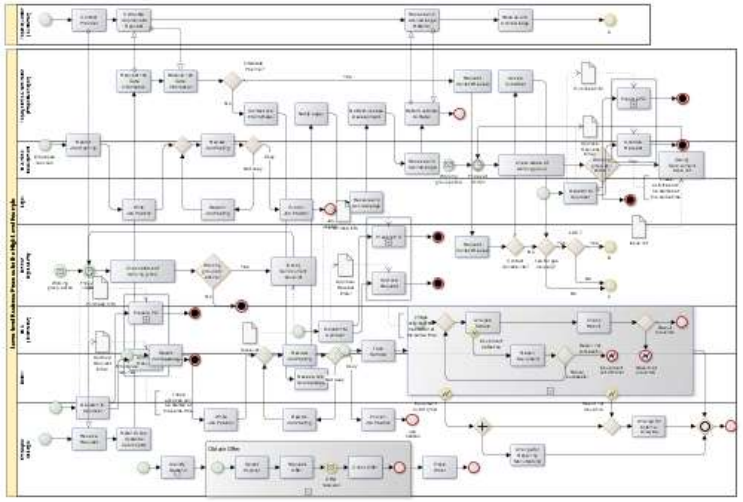
Black Risk – Zeitraum Entdeckung bis Veröffentlichung
Gray Risk – Zeitraum Veröffentlichung bis Verfügbarkeit eines Patches
White Risk – Zeitraum Verfügbarkeit eines Patches bis Implementierung

- Ungesicherter Kanal
- Zugriffskontrolle + Verschlüsselung
- Breaking-the-Glass Policy
- Rechtemanagement
- Back End
- <weitere Gegenmaßnahmen>
- <weitere Schwachstellen>

- **Cybersecurity Prozesse für:**
  - Analyse von Gefahren-Szenarien
  - Möglichkeiten von Angriffen (attack feasability, attack path, …)
  - Lieferantenmanagement
- **Regelmäßige Prüfung der Warn- und Informationsdienste**
  - CERT-Bund
  - "*Common Vulnerabilities and Exposures*" (CVE)
  - Oder andere "*Detection and Response Services*"
- **Prozesslandschaft zu komplex**
  - Alle Vorgaben wurden in Prozessen verankert
  - und nicht verzahnt mit anderen Tätigkeiten
    = eher ein Labyrinth



Reifegrad INFORMIERT



Security-
Vorfall

- **Beispiel – Prozesslandschaft**
  - Komplette Entwicklungsprozesse werden wiederholt

Updates(Programmer)

Updates(Pacemaker)

Software Delivery Network (SDN)

Programmer

Parametrierung

Updates(Pacemaker)

Patient

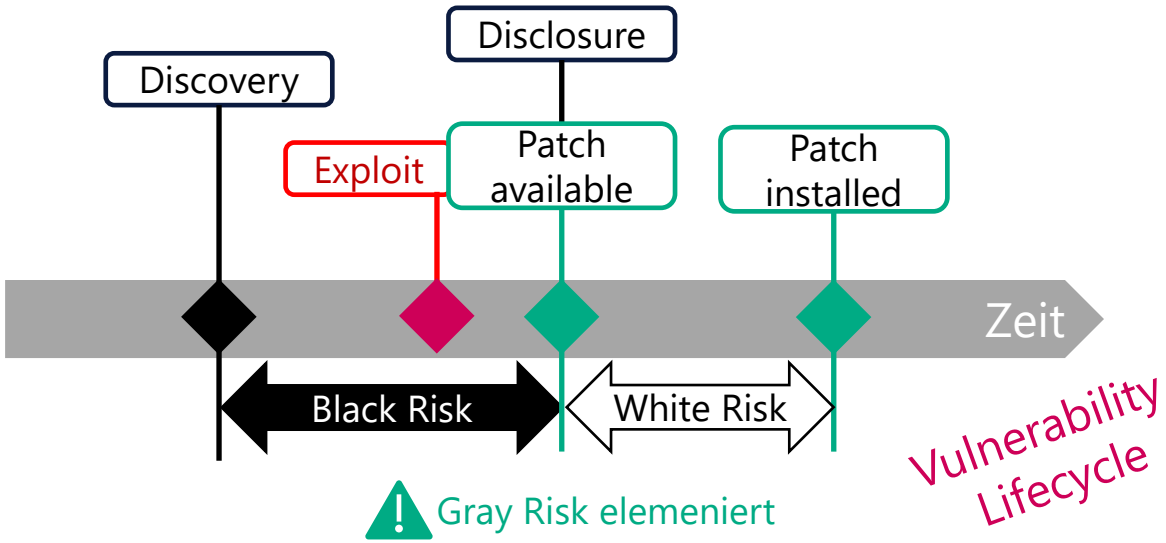
Pacemaker

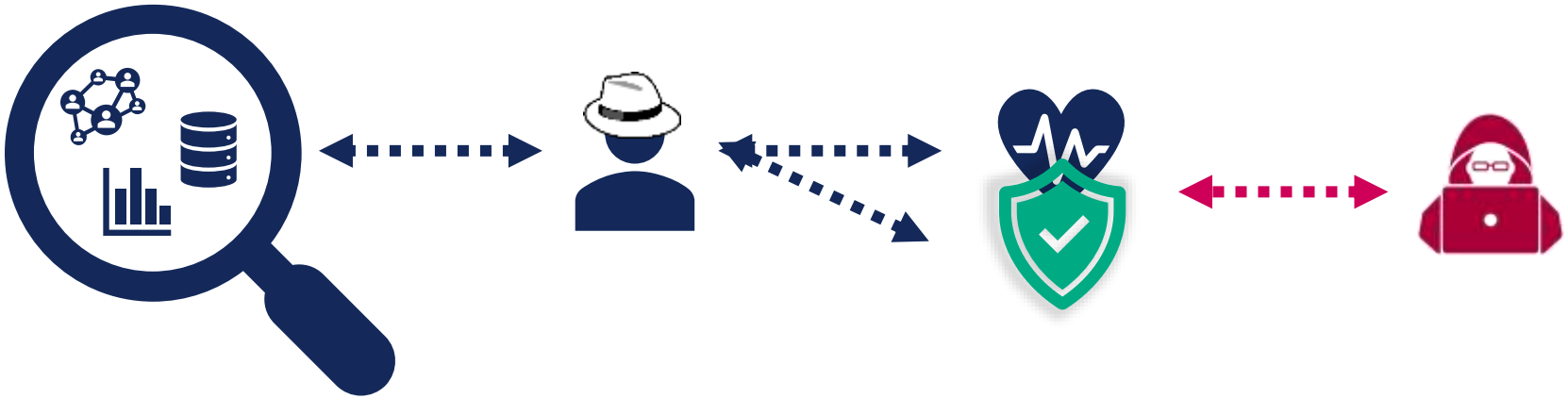
Reifegrad KOMPETENT

- **Die Zuständigkeiten für die Prozesse sind klar geregelt.**
- **Im Rahmen von Konzeptentscheidungen genießt die Cybersecurity immer die nötige Priorität.**
- **Verifikation und Validierung werden von ausreichend unabhängigen Mitarbeitern übernommen.**
- **Proaktives Handeln des Projekts bzw. der Mitarbeiter:**
  - Security by Design
  - Privacy by Design
- **Es sind ausreichend Ressourcen für die operative Arbeit vorhanden.**
- **Alle eingebundenen Mitarbeiter sind entsprechend ihren Aufgaben entsprechend geschult.**

Reifegrad KOMPETENT

- **Beispiel – Penetrationstests**
  - Regelmäßige Durchführung von Penetrationstests
  - Regelmäßige Adaptierung/Erweiterung von Tests basierend auf Monitoring und Nachforschungen
  - Proaktives härten der Technik
  - Potentielle Eliminierung der „Gray Risk“-Phase





Reifegrade – anderer Blickwinkel

Effizienz

Aspekt \ Reifegrad	Initial	Informiert	Kompetent
Reaktion auf Probleme	CAPA-Prozess (ohne Vorbereitung auf Cybersecurity)	Sehr detaillierte Arbeitsanweisungen	Anpassbare Arbeitsanweisungen, Adaptive Reaktion
Cybersecurity-Prozess	Pro forma Prozesse	Prozesslandschaft (Zu Komplex)	Lebende Prozesslandschaft Mit Messung und KVP
Incident-Management	Einmal im Quartal Prüfung der Warn- und Informationsdienste	tägliche Prüfung der Warn- und Informationsdienste	Wie informiert
PEN Test	Automatisierte Vulnerability Scans	Nach Standards testen (u.a. IEC 62443), Testen von bekannten Vulnerabilities (öffentlich bekannt)	Wiederholte PENtests mit aus Marktbeobachtung erstellten Test-Suits
Kontinuierlicher Verbesserungsprozess (KVP)	KVP wird Pro forma für die Zertifizierung durch geführt	KVP wir einmal im Jahr durchgeführt	Verbesserungen werden ständig erfasst und zu regelmäßigen Terminen im KVP
Return on Invest	Keine Investitionen	Viele Aktivitäten kosten viel Geld	Performant, Fokussiert
Risiken	Probleme, die am Markt bereits bekannt sind, werden zu Risiken. Sehr lange „Gray Risk" Phasen.	Durch komplexe Prozesslandschaft unnötig lange „Gray Risk" Phasen	Aufgrund Marktbeobachtung Reduzierung der potentiellen Probleme

Zusammenfassung

Medizingeräte

- Medizingeräte (IoT, auch implantiert) sind ggf. lebenswichtig
- Schnittstellen (Connectivity) …
  - … ermöglicht coole Funktionen
  - … ist medizinisch essentiell (und Wartung!)

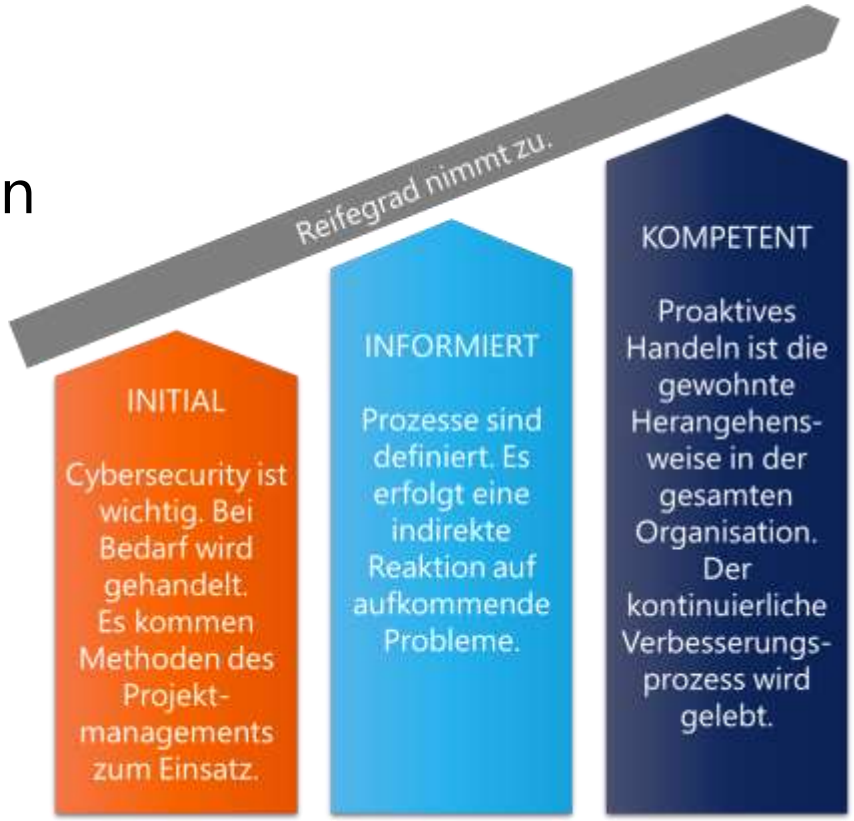
Angriffe

- Angriffe der Medizingeräte über die Schnittstellen
- Zulassung bedarf Cybersecurity-Betrachtungen
- „Security machen“ ist nicht ausreichend

Cybersecurity-Reife

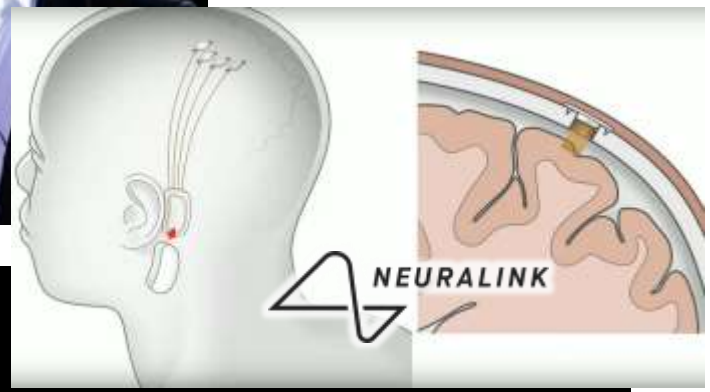
- Effizienz (und Effektivität) steigern
- Unternehmensrisiken senken

Kosten einsparen
Renomé erhalten

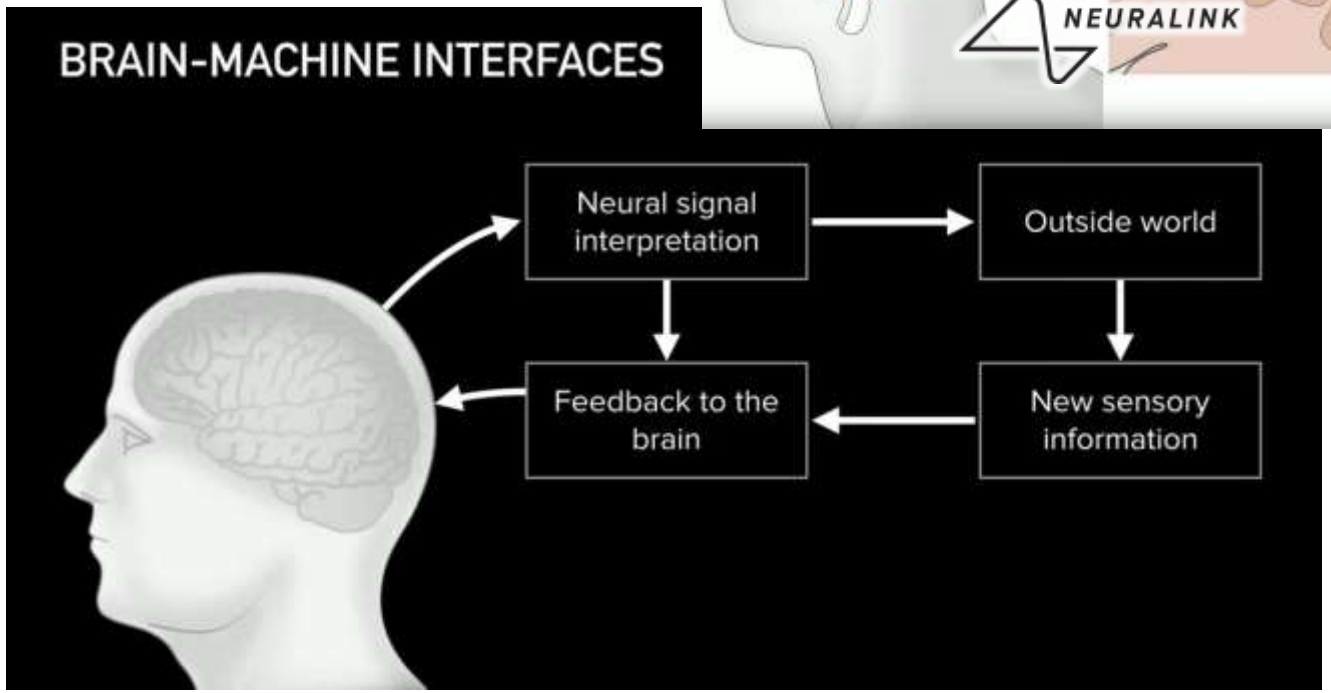


One for the road

Bildquelle: greatlakesledger.com



Bildquelle: abovetopsecret.com



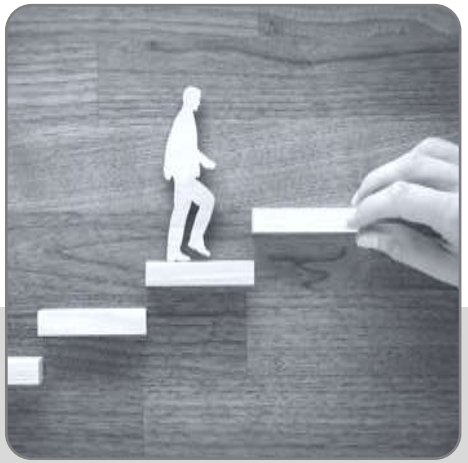
Bildquelle: medium.com - Neuralink Launch Event

- **Cybersecurity (Cyberdependability) frühzeitig beherrschen!**
- **Beispiel: Elon Musk ~ NEURALINK (www.neuralink.com)**

... und unsere Penetrations-Tester freuen sich schon auf ferngesteuerte Menschen

Wir sehen uns beim Vortrag: „A Way into Your **Head**"



Ihr Partner
für digitale Innovation.

cogitron
Verstand für Systeme

cogitron GmbH
Stefaniweg 4
85652 Pliening
Deutschland

Tel: +49 15 255 90 10 40
Fax: +49 89 20 35 15 53
info@cogitron.de
www.cogitron.de

HRB 234778 München
UStIdNr: DE 313 565 192