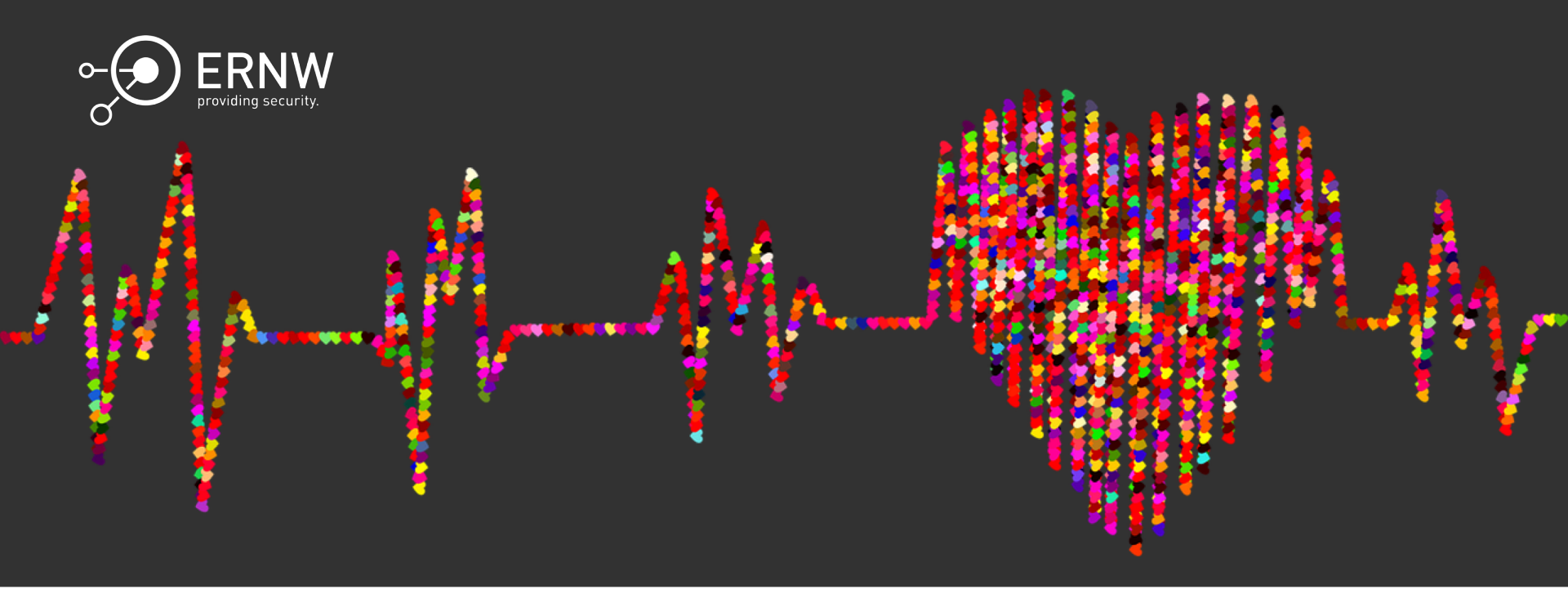
ERNW
providing security.



Die Sicherheit medizinischer Geräte
Das Spiel mit der Zeit

Julian Suleder, jsuleder@ernw.de

ERNW RESEARCH
pursuing knowledge.

@jsuleder

Julian Suleder

- M.Sc. Medizinische Informatik
- Security Analyst @ ERNW Research GmbH, Heidelberg
- Kontext:
  - Security Assessments für Krankenhäuser und Firmen
  - Prüfung von medizinischen Geräten sowie deren Integration in klinische Umgebungen, z.B. Patientenmonitore, Narkosegeräte, MRT
  - Prüfung von Krankenhausinfrastruktur
  - Erstellen von Konzepten für den sicheren Betrieb

ERNW
providing security.

Agenda

- Die Lage der IT-Sicherheit in medizinischen Umgebungen
- Beispiele für Schwachstellen in medizinischen Geräten
- Empfehlungen für Medizingerätehersteller
- Ausblick & weitere Forschung

ERNW RESEARCH
pursuing knowledge.

Das perfekte Ziel?

- Leistungserbringer verlassen sich bei der Bereitstellung ihrer Gesundheitsdienste auf IT
- Das Gesundheitswesen liegt beim Schutz seiner Infrastruktur hinter anderen Branchen:
  - Veraltete Technologien
  - Unsichere netzwerkfähige medizinische Geräte
  - Hersteller schieben Sicherheitsprobleme in die Verantwortung der Anwender


Photo by Annie Spratt on Unsplash

ERNW RESEARCH
pursuing knowledge.

NHS 2017: WannaCry

- Vor dem Angriff
  - Sicherheitsaudit für 88 von 236 Einrichtungen
  - Keine Einrichtung bestand die Prüfung
- Auswirkung des Angriffs
  - Störung des Betriebs in mindestens 34% der Einrichtungen
  - 1.220 infizierte Diagnosegeräte (1% aller Geräte)
  - Diagnoseausrüstung wurde entweder infiziert oder isoliert
  - 6.912 abgesagte Termine

[https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf, 2019-02-19]


Photo by Annie Spratt on Unsplash

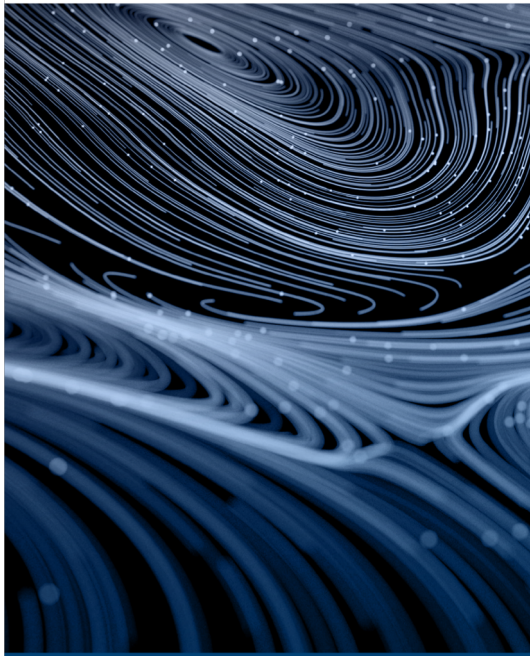
ERNW RESEARCH
pursuing knowledge.

BSI: Die Lage der IT-Sicherheit in Deutschland

- 2018:
  - Kontinuierlich steigende Anzahl vernetzter Medizingeräte auf dem deutschen Markt
  - Angriffe mit potenziellen Bedrohungen für die Patientensicherheit nehmen zu
  - Kompromiss: Med. Funktionalität vs. Sicherheit
  - Sicherheit von Medizinprodukten soll durch gezielte Forschungsprojekte analysiert werden

[https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html, 2019-02-19]

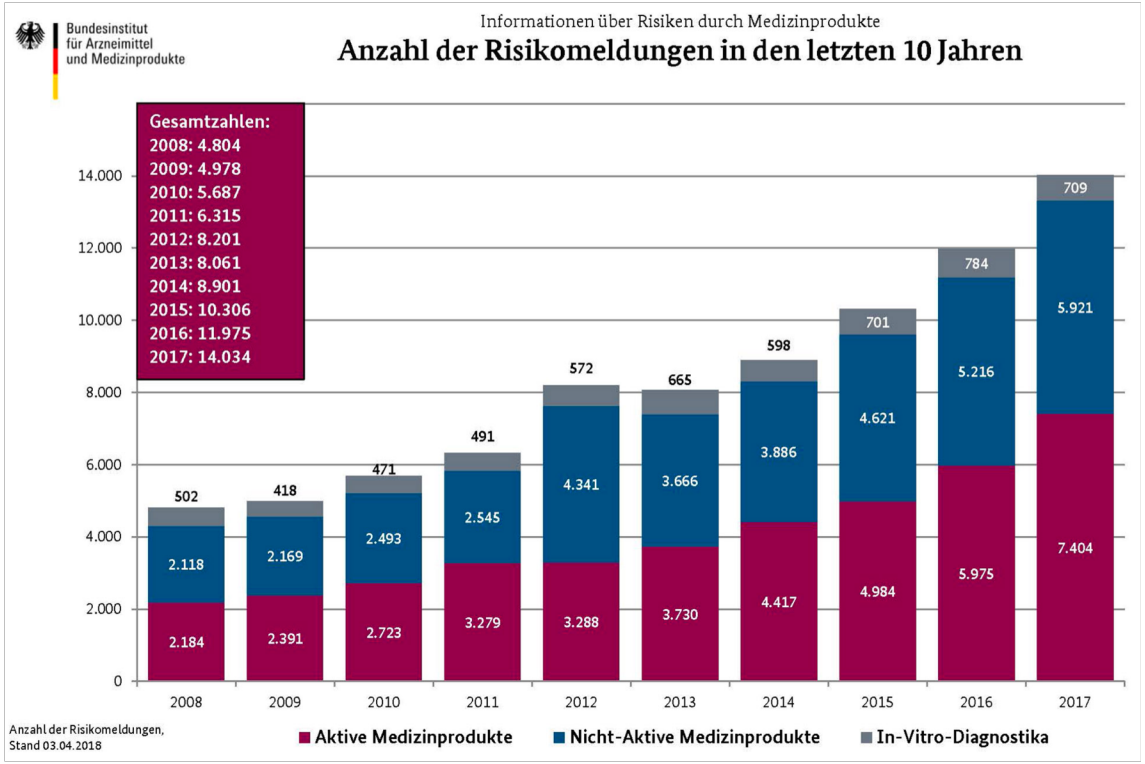
Federal Office
for Information Security



The State of IT Security in Germany 2018

Statistiken des BfArM

- Steigende Anzahl der Risikomeldungen
- 2017: 20 Meldungen/d
- Bias:
  - Änderungen in der Umgebung?
  - Größeres Bewusstsein Vorfälle zu Melden?

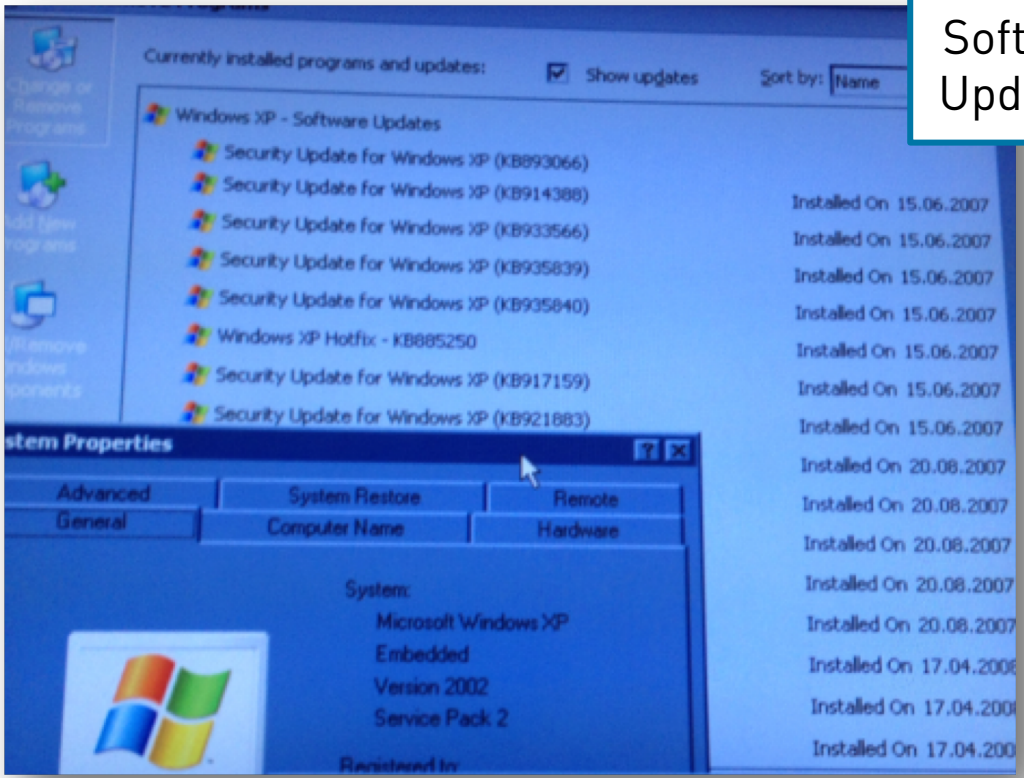


[https://www.bfarm.de/DE/Service/Statistiken/MP_statistik/AllgStatAngaben/Anzahl-Risikomeldungen/_node.html, 2019-03-10]

Photo by Sara Bakhshi on Unsplash

Beispiele unsicherer Medizingeräte

Ultraschallgerät (2017)



Software Updates?

ERNW RESEARCH
pursuing knowledge.

Ziel: Infusionspumpe

- Innerhalb des Krankenhauses „beweglich“
- Intravenöse Zufuhr von z.B. Medikamenten
- Häufig durch eine zentrale Verwaltungssoftware im Krankenhaus gesteuert

[https://ics-cert.us-cert.gov/advisories/ICSA-15-125-01B, 2019-04-03]

ERNW RESEARCH
pursuing knowledge.

Ziel: Infusionspumpe

- Problem 1: Unauthentifizierte Schnittstelle
  - Root Privilegien auf Port 23/TELNET
  - Benutzer: `root`, Password `<empty>`
- Voraussetzungen:
  - Netzwerkzugriff über z.B. LAN-Anschlüsse am Bett
  - Angreifer mit niedrigem Skill-Level
- Alle Pumpen befinden sich im gleichen Netzwerk
- → Ein Angreifer entdeckt alle Pumpen

[https://ics-cert.us-cert.gov/advisories/ICSA-15-125-01B, 2019-04-03]

ERNW RESEARCH
pursuing knowledge.

Ziel: Infusionspumpe

- Problem 2: Unkontrollierter Ressourcenverbrauch
  - Überlastung durch zu viele TCP-Pakete
  - Unauthentifiziert
- Voraussetzungen:
  - Netzwerkzugriff
  - Angreifer mit niedrigem Skill-Level
- Auswirkung
  - Gerät ist funktionsunfähig
  - Manueller Neustart des Geräts erforderlich

[https://ics-cert.us-cert.gov/advisories/ICSA-15-125-01B, 2019-04-03]

ERNW RESEARCH
pursuing knowledge.

Ziel: Infusionspumpe

- Problem 3: Vertrauen in nicht autorisierte Quellen
  - Keine Prüfung der Authentizität der empfangenen Daten und kommunizierenden Hosts
- Angriff:
  - Manipulation von Medikamentenbibliotheken, Softwareupdates oder Gerätekonfigurationen
- Voraussetzung
  - Der Angreifer muss semantisch gültige Daten senden
  - Angreifer mit mittlerem Skill-Level

[https://ics-cert.us-cert.gov/advisories/ICSA-15-125-01B, 2019-04-03]

ERNW
providing security.

Publikumsfrage:

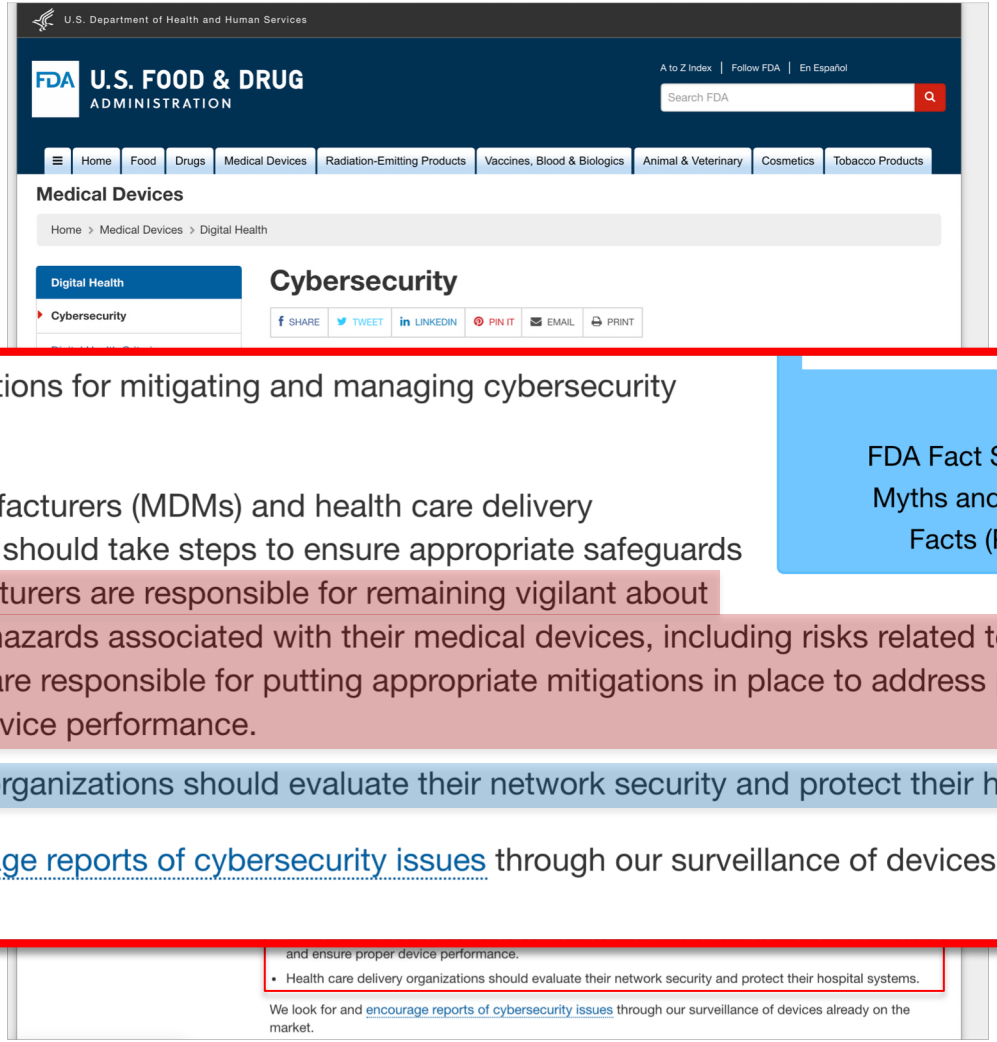
- Wer ist für die Überprüfung der Sicherheit (Security) von Medizinprodukten zuständig?
  - Das Bundesamt für Sicherheit in der Informationstechnik (BSI)
  - Die an der Zulassung beteiligten Stellen
  - Der Hersteller
  - Der Anwender / Patient
  - Niemand

ERNW
providing security.

Photo by Joshua Coleman on Unsplash

Empfehlungen für die Sicherheit von Medizingeräten

ERNW RESEARCH
pursuing knowledge.



The FDA's recommendations for mitigating and managing cybersecurity threats include:

- Medical device manufacturers (MDMs) and health care delivery organizations (HDOs) should take steps to ensure appropriate safeguards are in place. Manufacturers are responsible for remaining vigilant about identifying risks and hazards associated with their medical devices, including risks related to cybersecurity. These organizations are responsible for putting appropriate mitigations in place to address patient safety risks and ensure proper device performance.
- Health care delivery organizations should evaluate their network security and protect their hospital systems.

We look for and encourage reports of cybersecurity issues through our surveillance of devices already on the market.

FDA Fact Sheet: Dispelling Myths and Understanding Facts (PDF - 175kb)

https://www.fda.gov/medicaldevices/digitalhealth/ucm373213.htm

ERNW RESEARCH
pursuing knowledge.

Entwurf

FDA: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

- Zielgruppe: Hersteller medizinischer Geräte vor der Zertifizierung
- Unterschiede zur Version von 2014:
  - Ausführliche Dokumentation für Design und Implementierung
  - Die Sicherheit von Medizinprodukten ist gemeinsame Verantwortung
  - Risikobewertung während des gesamten Produktlebenszyklus
- Cybersecurity Bill of Materials (CBOM)

[https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM623529.pdf, 2019-03-10]

ERNW RESEARCH
pursuing knowledge.

BSI CS-132: Cyber-Sicherheitsanforderungen an netzwerkfähige Medizinprodukte

- Best Practices für Hersteller vernetzter medizinischer Geräte
- Ergänzung und Begleitung regulatorischer Anforderungen
- Unterscheidung nach Betriebsarten
  - Medizinischer Zweck
  - Gerätekonfiguration (inkl. patientenspezifischer Parameter)
  - Technische Wartung (Updates + Kalibrierungen oder Anpassungen)
- Sicherheitsmaßnahmen dürfen die Safety der Medizinprodukte und damit das Leben der Patienten nicht negativ beeinflussen

[https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_132E.html, 2019-03-10]

ERNW
providing security.

Ausblick & weitere Forschung

ERNW RESEARCH
pursuing knowledge.

ManiMed: Manipulation von Medizinprodukten

- Öffentliche Ausschreibung des BSI
- Zeitrahmen: 18 Monate
- Ziel: Sensibilisierung von Herstellern und der Bevölkerung bezüglich der IT-Sicherheitsrisiken von vernetzten Medizinprodukten
- Inhalte:
  - Einschätzung der Marktlage vernetzter Medizinprodukte
  - Analyse der IT-Sicherheit dieser Produkte durch Security Assessments
  - Veröffentlichung der Sicherheitsanalyse

ERNW RESEARCH
pursuing knowledge.

Referenzen

- **Julian Suleder, Dr. Andreas Dewald, Florian Grunow**; ERNW Whitepaper 66: Medical Device Security: A Survey of the Current State; Online: https://ernw.de/en/whitepapers/issue-66.html; 2018.

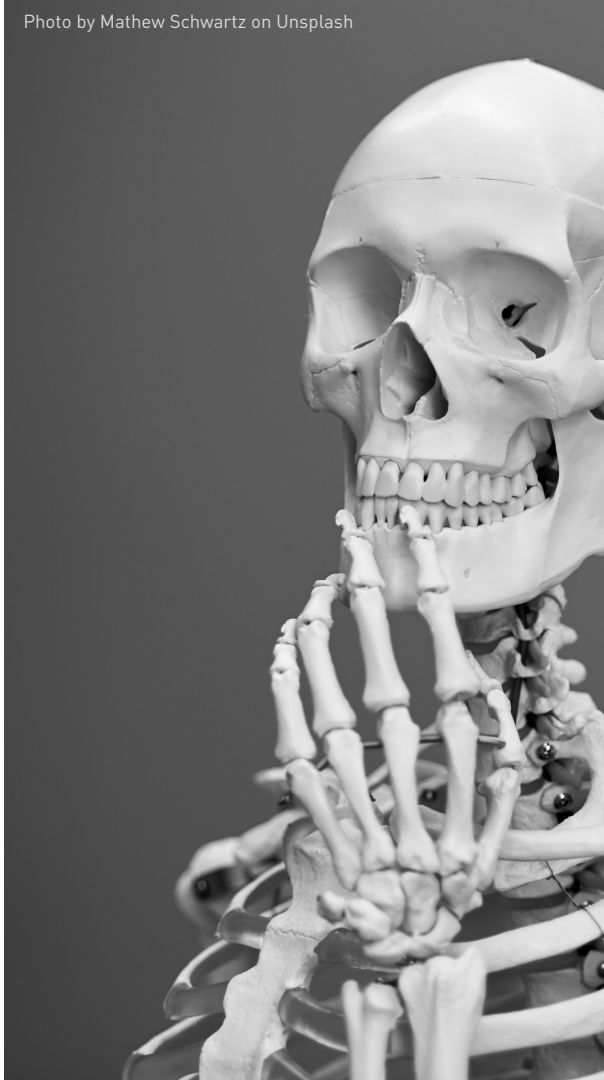


Photo by Mathew Schwartz on Unsplash

ERNW RESEARCH
pursuing knowledge.

Vielen Dank für Ihre Aufmerksamkeit!

Zu Risiken und Nebenwirkungen fragen Sie Ihren Arzt oder Apotheker.

jsuleder@ernw.de

@jsuleder

www.ernw.de

www.insinuator.net