ehealth summit austria

HIMSS Europe

In Kooperation mit

HEALTH 2016

eHEALTH 2016 www.eHealth2016.at

Informationssicherheit und Datenschutz als Chance

Wie Sie durch ein angemessenes Sicherheitsniveau Ihre IT-Risiken senken und trotzdem effizient weiterarbeiten können

ehealth summit austria

HIMSS Europe

In Kooperation mit

HEALTH 2016

eHEALTH 2016 www.eHealth2016.at

Hauptprobleme in der Informationssicherheit

- Passwörter
- Sicherheitsbewusstsein der Mitarbeiter
- Sicherheitsvorgaben und Kontrollen
- Ransomware

ehealth summit austria

HIMSS Europe

In Kooperation mit

HEALTH 2016

eHEALTH 2016 www.eHealth2016.at

Gibt es überhaupt ein “sicheres” Passwort?

Anforderungen an „sichere“ Passwörter

- **Mindestlänge**: 10 Zeichen
- **Komplexität** (Kombination aus Groß-, Kleinbuchstaben, Ziffern und Sonderzeichen)
- **Regelmäßiges Ändern** der Passwörter
- Vermeidung von **Privatbezug** (z.B. Geburtstag)
- Vermeidung von **Wörtern aus Wörterbüchern**
- Trennung zwischen **Privat- und Firmenpasswörtern**
- Unterschiedliche Passwörter **je Applikation** (vor allem im Internet problematisch) usw.

Fazit

- Anforderungen an sichere Passwörter sind **nicht praxistauglich**!
- Umgang mit Passwörtern ist in der Regel unsicher!

ehealth summit austria

HIMSS Europe

In Kooperation mit

HEALTH 2016 eHEALTH 2016 www.eHealth2016.at

Gibt es Alternativen zu Passwörtern?

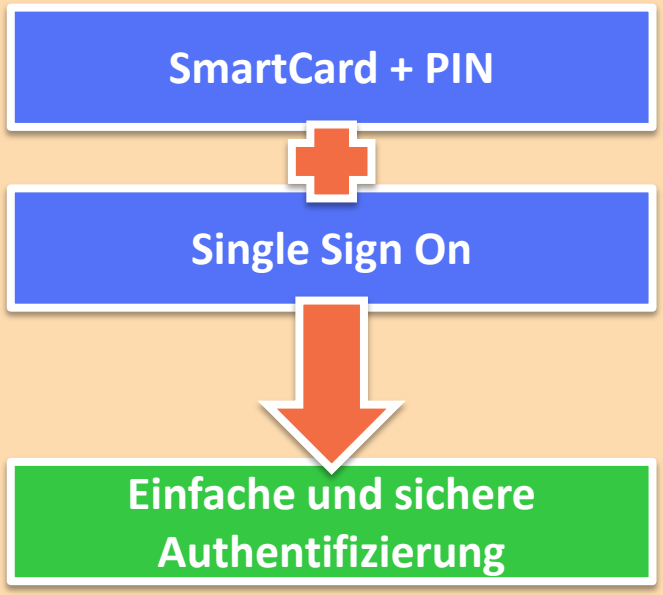
Einsatz von SmartCards

- Karte mit PIN
- 2-Faktor-Authentifizierung (**Besitz, Wissen**)
- Breit akzeptiertes Verfahren
- Ändern des PINs nur im Verdachtsfall
- Sicherer als jedes Benutzer-/Passwortverfahren
- Kann Passwörter nicht zu 100% ablösen

Merkhilfen

- Ich fahre gerne jeden 2. Sonntag mit meinem Oldtimer!
- **Passwort: Ifgj2SmmO!**

Passwort Manager



ehealth summit austria

HIMSS Europe

In Kooperation mit

HEALTH 2016

eHEALTH 2016 www.eHealth2016.at

Wie schule ich meine Mitarbeiter?

Der Faktor Mensch ist das größte Sicherheitsrisiko!

- Fehler (unabsichtlich / absichtlich)
- Bequemlichkeit
- Social Engineering
- Phishing

Kreative Möglichkeiten zur regelmäßigen Schulung!

- Goodies mit Sicherheitshinweisen
- Workshops, Plakate, Checklisten
- Awareness App auf Smartphone
- Onboarding-Kurse, Paten-Regelungen, Welcome-Mappen
- eLearning

Bildquelle: findicons.com

ehealth summit austria

HIMSS Europe

In Kooperation mit

HEALTH 2016

eHEALTH 2016 www.eHealth2016.at

Praxisbeispiel: eLearning

Frage 1

Richtig

Erreichte Punkte 1,00 von 1,00

Frage markieren

Welche Daten dürfen nicht versendet werden?

Wählen Sie eine oder mehrere Antworten:

- [ ] a. Fiktive medizinische Daten
- [x] b. Medizinische Daten
- [x] c. Patientendaten
- [x] d. Personenbezogene und/oder sensible Daten
- [ ] e. Anonymisierte Patientendaten

Die richtige Antwort lautet: Personenbezogene und/oder sensible Daten, Medizinische Daten, Patientendaten

Frage 2

Richtig

Erreichte Punkte 1,00 von 1,00

Frage markieren

Folgendes Szenario: Für eine Fehleranalyse ist es dringend notwendig, dass du einen Datenbank-Auszug mit personenbezogenen Daten an einen Hersteller versendest. Eine Anonymisierung der Daten ist jedoch aufgrund von unvertretbar hohem Aufwand nicht möglich. Wie gehst du vor?

Wählen Sie eine oder mehrere Antworten:

- [x] a. Ich weiß, dass personenbezogene und sensible Daten vor jedem Versand nach extern zwingend anonymisiert werden müssen. Da die Anonymisierung der Daten jedoch nicht möglich ist, hole ich vor der Datenübertragung eine schriftliche Genehmigung vom IT-Sicherheitsbeauftragten ein.
- [ ] b. Ich weiß, dass lediglich sensible Daten vor jedem Versand nach extern zwingend anonymisiert werden müssen. Personenbezogene Daten darf ich jederzeit und ohne vorheriger Anonymisierung nach extern versenden.
- [ ] c. Da die Fehleranalyse dringend erfolgen muss, darf ich die Daten trotz Personenbezug ausnahmsweise nach extern versenden.

Die richtige Antwort lautet: Ich weiß, dass personenbezogene und sensible Daten vor jedem Versand nach extern zwingend anonymisiert werden müssen. Da die Anonymisierung der Daten jedoch nicht möglich ist, hole ich vor der Datenübertragung eine schriftliche Genehmigung vom IT-Sicherheitsbeauftragten ein.

ehealth summit austria

HIMSS Europe

In Kooperation mit

HEALTH 2016

eHEALTH 2016 www.eHealth2016.at

Sicherheitsvorgaben und Kontrollen

Schriftliche Vorgaben!
- IT-Sicherheitsrichtlinie
- IT-Benutzerrichtlinie
- Datenschutzrichtlinie

Kontrolle von schriftlichen Vorgaben!
- Richtlinien ohne Kontrolle sind wertlos

Inhalt von Richtlinien
- Management Commitment
- Definition von Verantwortlichkeiten
- Nutzung von Internet und E-Mail
- Umgang mit Unternehmenseigentum
- Privatnutzung von IT-Systemen
- Datenschutzbestimmungen
- Umgang mit IT-Sicherheitsproblemen und Notfällen
- Schulungsmaßnahmen
- Umgang mit Risiken usw.

ehealth summit austria

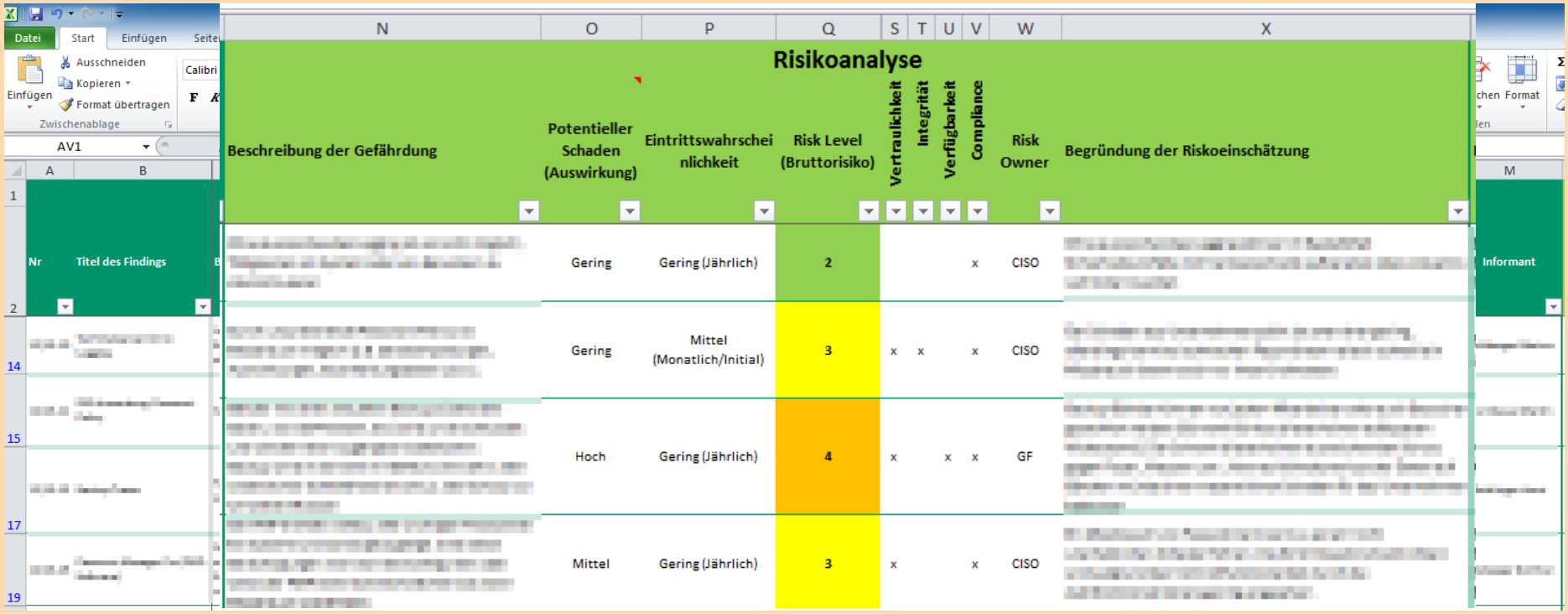
HIMSS Europe

In Kooperation mit

HEALTH 2016

eHEALTH 2016 www.eHealth2016.at

Praxisbeispiel: IT-Risikomanagement



Nr	Titel des Findings	Beschreibung der Gefährdung	Potentieller Schaden (Auswirkung)	Eintrittswahrscheinlichkeit	Risk Level (Bruttorisiko)	Vertraulichkeit	Integrität	Verfügbarkeit	Compliance	Risk Owner	Begründung der Riskoeinschätzung	Informant
					Risikoanalyse							
			Gering	Gering (Jährlich)	2				x	CISO		
14			Gering	Mittel (Monatlich/Initial)	3	x	x		x	CISO		
15			Hoch	Gering (Jährlich)	4	x		x	x	GF		
17			Mittel	Gering (Jährlich)	3	x			x	CISO		

ehealth summit austria

HIMSS Europe

In Kooperation mit

HEALTH 2016

eHEALTH 2016 www.eHealth2016.at

Praxisbeispiel: IT-Risikomanagement

AJ	AK	AL	AM	AN	AO	AQ	AR	AS	AT	AU
Entscheidung zur Risikobehandlung					Implementierung	Performance-Evaluierung				
Entscheidung	Entscheider	Risikobehandlungs-Priorität	Typ der Risikobehandlung	Entscheidungs-datum	Geplante Fertigstellung	Beschreibung der Überprüfung	Datum der Überprüfung	Intervall der Performance-Evaluierung	Prüfergebnis	Erledigt am (Datum)
[illegible]	[illegible]	3 - Mittel	Reduktion	16.12.2014	[illegible]	[illegible]	[illegible]	[illegible]		
[illegible]	[illegible]	3 - Mittel	Reduktion	06.02.2015	[illegible]	[illegible]	[illegible]	[illegible]		
[illegible]	[illegible]	4 - Gering	Reduktion	07.05.2015	[illegible]	[illegible]	[illegible]			
[illegible]	[illegible]	4 - Gering	Reduktion	07.05.2015	[illegible]	[illegible]	[illegible]	[illegible]		

Präsentiert von

HIMSS Europe

AIT Austrian Institute of Technology TOMORROW TODAY

Österreichische Gesellschaft für Biomedizinische Technik Austrian Society for Biomedical Engineering

OESTERREICHISCHE COMPUTER GESELLSCHAFT AUSTRIAN COMPUTER SOCIETY

UMIT

ehealth summit austria

HIMSS Europe

In Kooperation mit

HEALTH 2016

eHEALTH 2016 www.eHealth2016.at

Ransomware

- **Application Whitelisting**
- **Network Security Features**
- **Backup** (Pull-Verfahren)
- **Berechtigungen einschränken**
- **Sofortmaßnahmen** (NW-Kabel, Read Only, Checkliste)
- **Security Awareness**

Bekannte Applikationen

Unbekannte Applikationen

Bildquelle: findicons.com

ehealth summit austria

HIMSS Europe

In Kooperation mit

HEALTH 2016

eHEALTH 2016 www.eHealth2016.at

Fazit

- Informationssicherheit und Datenschutz können **nicht mehr ignoriert** werden!
- Erlassen Sie **schriftliche Vorgaben**!
- Definieren Sie **Verantwortlichkeiten**!
- Identifizieren Sie Ihre **IT-Risiken**!
- Ergreifen Sie **angemessene technische und organisatorische Maßnahmen**!
- **Schulen** Sie Ihre Mitarbeiter!
- **Kontrollieren** Sie stichprobenartig die Einhaltung der Vorgaben!

Informationssicherheit ist keine Zustand, sondern ein Prozess!