Faktor Mensch die Achillesferse der IT-Sicherheit

September 2020

KONVERTO

Martin Galler

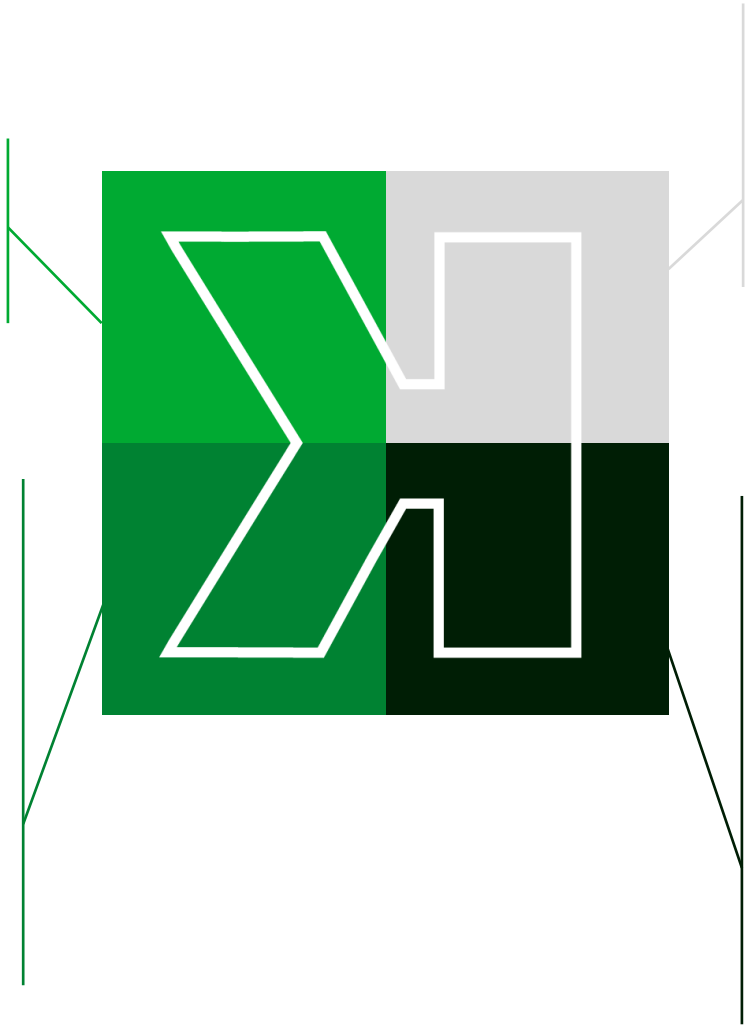
Privacy & Data Security

martin.galler@konverto.eu

KONVERTO

Figures | Data | Facts

Datacenter:
1.500 virtual server
2.500 virtual workplace
10 TB RAM
400 TB SSD storage



managed network devices:
~ 1.000 router
~ 1.700 switches
~ 700 access points
~ 600 firewalls

Connectivity:
3.550 km Glasfaser-Backbone
~ 200 POP
150 Funk-POP
16.000 Breitbandanschlüsse

Security:
~ 4.500 automatisch analysierte LOG-Zeilen pro Sekunde

~ 100.000 blockierte Verbindungs-versuche pro Woche zu Malware, Phishing und Spam Domains

KONVERTO

Schutzmaßnahmen klassisch

- Next Generation Firewall
- Content Filter fürs Internet
- Endpoint Protection
- Spam Filter
- Backup
- Systeme updaten
- Starkes Passwort
- Ordentliche Zugangsberechtigungen

- Vertrauenswürdige Software
- Saubere Konfiguration der Systeme
- Physische Sicherheit
- Sicherer Fernzugang

KONVERTO

Aktueller Exkurs: Systeme updaten

Hacker-Angriff auf Uniklinik Düsseldorf
Ermittlungen wegen fahrlässiger Tötung
17. September 2020, 16:37 Uhr dpa

Nach einem Erpressungsversuch der Uniklinik Düsseldorf durch Hacker kam eine Patientin ums Leben. Gegen die Täter wird nun auch wegen fahrlässiger Tötung ermittelt.

KONVERTO

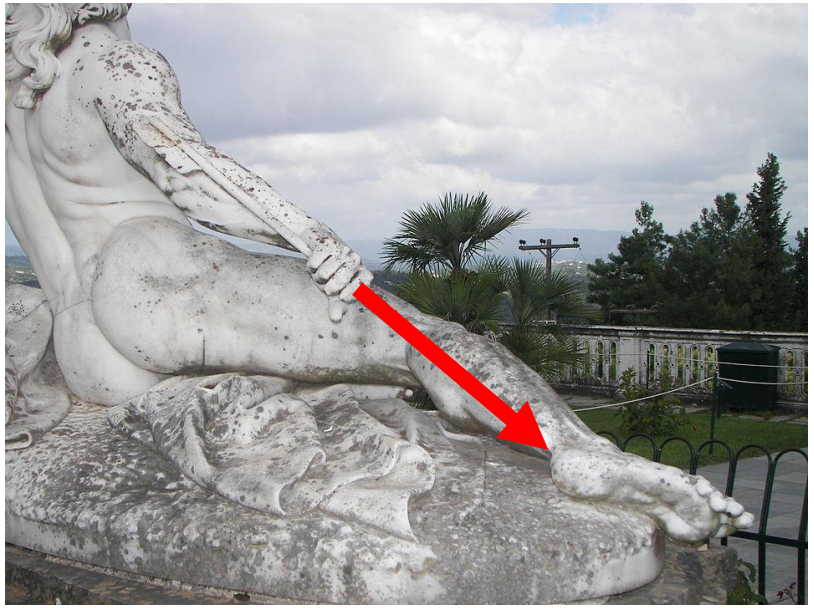
Schutzmaßnahmen modern

- Sicherheit mobile Geräte
- Sichere Authentifizierung (MFA)
- Sichere Apps
- Sichere Cloud
- Risikobasierte Zugriffssteuerung
- User Behavior Analysis mit KI
- Advanced Threat Protection
- Sicheres Homeoffice

KONVERTO

Social Engineering

Angriffsziel Mensch



Tasoskessaris presunto CC BY-SA 3.0,
https://commons.wikimedia.org/w/index.php?curid=1443008

KONVERTO

Was ist Social Engineering?

- Manipulation von Personen
- Auslösen von Fehlverhalten
- Ausnutzung von Emotionen
- Psychologische Tricks
- Unterstützung durch digitale Kommunikation

KONVERTO

Wählen Sie die beste Antwort

Sie erhalten eine dringende Nachricht von Ihrer Bank. Darin heißt es, dass Ihr Konto aufgrund unberechtigter Zugriffsversuche gesperrt wurde. Angeblich müssen Sie das Passwort zurücksetzen, um Ihre Gelder wieder mithilfe eines beigefügten Links zu entsperren. Was sollten Sie tun?

- Sie klicken auf den Link in der E-Mail und setzen Ihr Kennwort zurück.
- Sie gehen zur Haupt-Internetseite der Bank und melden sich dort an, um Ihr Konto zu überprüfen.
- Sie antworten auf die E-Mail und bitten um Bestätigung, dass die Aufforderung legitim ist.
- Sie rufen die Nummer in der E-Mail an und erledigen die Angelegenheit telefonisch.

KONVERTO

Als Sie ein Konferenzzimmer betreten, finden Sie auf dem Tisch ein USB-Speichergerät. Sie schließen es an Ihren Arbeits-Laptop an, um zu sehen, ob es Informationen enthält, anhand derer Sie den Besitzer identifizieren können.

Schlechte Entscheidung

Gute Entscheidung

KONVERTO

Alexa, eine Buchhalterin, erhält folgende E-Mail. Sie vergewissert sich, dass die Absenderadresse dem Geschäftsführer gehört, und sendet das Geld.

Von: MSilberstein@wlcglobal.com
Betreff: DRINGENDE BITTE: Überweisung

Überweisen Sie sofort 17.380,00 € an unseren Anwalt, um unseren Schuldensaldo zu begleichen. Die Informationen finden Sie nachstehend.

Riskant

Sicher

KONVERTO

Menschliche Eigenschaften im Fokus

- Vertrauen
- Hilfsbereitschaft
- Freundlichkeit
- Dankbarkeit
- Stolz auf die Arbeit und den Betrieb (Loyalität)
- Streben nach Anerkennung und Lob
- Angst

- Autoritätsglaube
- Neugier
- Bequemlichkeit-Trägheit
- Oberflächlichkeit
- Angeberei und Geschwätzigkeit

Passwort

KONVERTO

Top 20 deutscher Passwörter:

1	123456	11	dragon
2	123456789	12	iloveyou
3	12345678	13	password1
4	1234567	14	monkey
5	password	15	qwertz123
6	111111	16	target123
7	1234567890	17	tinkle
8	123123	18	qwertz
9	000000	19	1q2w3e4r
10	abc123	20	222222

Situation Deutschland 2019, Studie Hasso Plattner Institut, 67 Millionen Zugangsdaten

KONVERTO

Unternehmens-Passwort

Bisherige Passwortrichtlinien

- Passwortlänge
- Komplexität (Groß-/Kleinbuchstaben, Ziffern, Sonderzeichen)
- Erzwungene Passwortänderung
- Kein "Passwort Recycling"

Neue Erkenntnisse:

- Keine regelmäßige erzwungene Passwortänderung
- Passwortlänge erhöhen
- Wenn möglich **2-Faktor-Authentisierung**
- Blacklist von trivialen Passwörtern

KONVERTO

Private Passwörter

Pro System ein eigenes Passwort

Darf **niemals Unternehmenspasswort** sein

Passwörter nicht im Browser speichern

Hilfestellung: vertraulicher Passwortmanager

Neue Möglichkeiten:

- Biometrische Verfahren
- Passwordless (FIDO2)

KONVERTO

Phishing

KONVERTO

Phishing - die Gefahren

Gefahren

- Bösartige Links
- Bösartige Anhänge
- Anfragen für sensible Daten

KONVERTO

Phishing - die Kunst der Täuschung

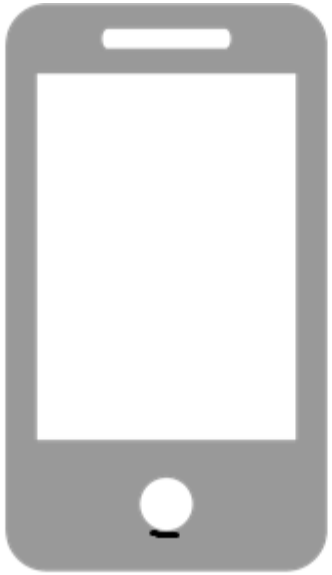
Psychologische Tricks

- Bekannte Personen/Institutionen vortäuschen
- Einschüchterungen/Angst/Druck erzeugen
- Aufregende Versprechen machen

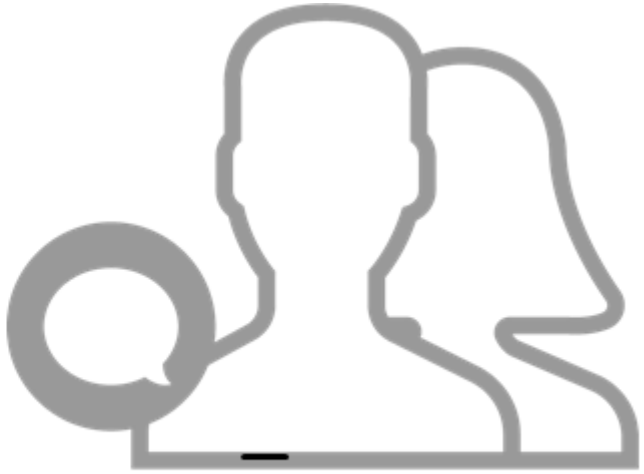
Phishing – nicht nur E-Mail

SMS/text phishing
(“smishing”)

Voice phishing
(“vishing”)



Social media phishing
(über Fake-Konten und böswillige Posts)



KONVERTO


20:35
Banca MPS
SMS-Nachricht
Heute, 20:31
Ci risultano delle spese sospette sul suo conto, il servizo antifrode consiglia di verificare il conto per evitarne la sospensione https://direttiva-banca.com


18:03
Gruppo ISP
SMS-Nachricht
Heute, 17:59
Dopo alcuni controlli sono emersi pagamenti sospetti provenienti dal suo conto confermi i suoi dati per evitarne il blocco https://banca-intesa-italia.com

KONVERTO

Warum ist Phishing so „beliebt“?

- Einfach
- Billig
- Effektiv – es funktioniert
- Allgemeine Angriffe und personalisierte Angriffe

- Kriminelle erhalten damit
  - Direkt Geld
  - Zugang zu Konten (Bank, E-Mail, Social Media)
  - Kontaktnamen und Kundenlisten
  - Wichtige Firmeninformationen
  - Server, Systeme und Netzwerke

KONVERTO

Welchen Schaden richtet Phishing an?

Privat

- Geld vom Konto gestohlen
- Betrügerische Belastungen von Kreditkarten
- In Ihrem Namen eröffnete Darlehen
- Shopping von Ihrem Konto
- Verlust von Fotos, Videos etc.
- Gefälschte Social Media Posts

Beruflich

- Verlust von Geld
- Offengelegte persönliche Informationen von Kunden
- Zugang von Externen zu vertraulichen Informationen
- Gesperrte Files

KONVERTO

Abwehr von Phishing - 1

E-Mails gründlich lesen

- Rechtschreibfehler, schlechte Grammatik
- Stimmt der Ton
- Unaufgeforderte E-Mails

Fragen

- Erwarte ich ein solche E-Mail?
- Macht diese E-Mail Sinn?
- Werde ich zu schnellem Handeln gedrängt?
- Zu gut um wahr zu sein?

KONVERTO

Abwehr von Phishing - 2

Sender überprüfen

- Verwendung von bekannten Logos
- Falsche Absenderadresse vorgetäuscht
- Bei kompromittierten Accounts wird sogar die korrekte Absenderadresse verwendet

Nachfragen

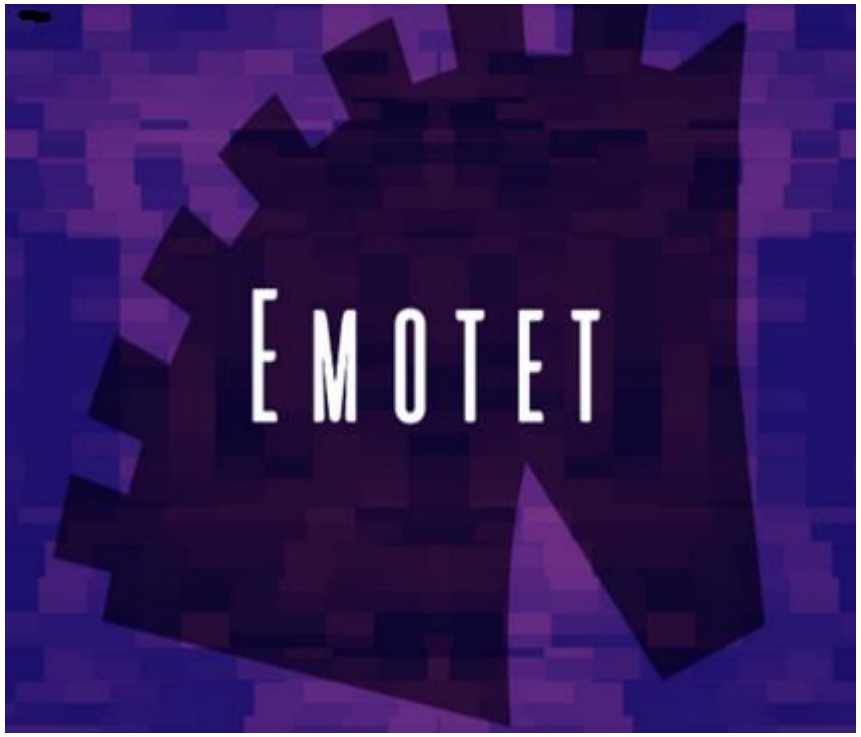
- In der IT-Abteilung
- Beim Absender

KONVERTO

Beliebte Phishing Themen

- Paketzustellung
- Rechnungszustellung
- Aktuelle Themen: COVID-19
- Stellenbewerbungen
- Leere Emails nur mit Anhang
- Mail vom Kopierer/Scanner
- Voicemail
- Videokonferenz-Einladungen

KONVERTO



Momentan gefährlichste Schadsoftware

- Absender eigene Kontakte aus Outlook
- Inhalte eigene Konversationen aus Outlook
- **Betrüger schalten sich in real existierende Konversationen ein**

KONVERTO

Von Meier, Antje <compromised.account@extern.tld>☆
Betreff **RE: AW: Angemieteter Parkplatz Musterstraße**
An Mueller, Bertram <Bertram.Mueller@musterfirma.de>☆

anbei findest du den Überweisungsbeleg, das Geld sollte also bald bei dir auf dem Konto sein.
Ebenfalls anbei der Scan der Vereinbarung.bitte Anhang beachten.

http://musterfirma.de/doc/B-3256-UV5323/Musterfirma_0451742669_April_09_2019.doc

http://super-plus.pl/css/oo6a-atf3y-frzom/

Mit freundlichen Grüßen,
Meier, Antje
antje.meier@musterfirma.de

Sehr geehrte Frau Meier,

vielen Dank für die schnelle Bearbeitung.
Den Schlüssel für die Tiefgarage gebe ich dann in der Hausmeisterei zurück, nehme ich an.

Viele Grüße
Bertram Müller

Von Emotet zuvor auf infiziertem System ausgespähte authentische E-Mail

-----Ursprüngliche Nachricht-----
Von: Meier, Antje
Gesendet: Donnerstag, 28. Juni 2018 13:48
An: Müller, Bertram
Betreff: AW: Angemieteter Parkplatz Musterstraße

Sehr geehrter Herr Müller,

hiermit bestätige ich Ihnen den Eingang Ihrer Kündigung vom 28.06.2018.
Die Kündigungsbestätigung und den Stellplatzvertrag für den Stellplatz Nr. 42 erhalten Sie in den nächsten Tagen.

Mit freundlichen Grüßen
Im Auftrag

Antje Meier

Bild: CERT-Bund/BSI

Emotet - Folgen

- Angriffstechnik für gezielte (maßgeschneiderte) Angriffe ist nun allgemein verfügbar
- Der eigentliche Angriff erfolgt erst Wochen nach der Infektion
  - Arbeitsüberlastung der Angreifer
  - Zeit sich ein lohnendes Opfer auszusuchen
- Lösegeldforderungen im Steigen (6 bis 8-stellige Beträge)

KONVERTO

Soziale Netzwerke

KONVERTO

Elsa teilt nur den Tag und Monat ihres Geburtsdatums in einem sozialen Netzwerk

War das riskant oder sicher?

Riskant	Sicher

KONVERTO

Gefahren durch soziale Netzwerke

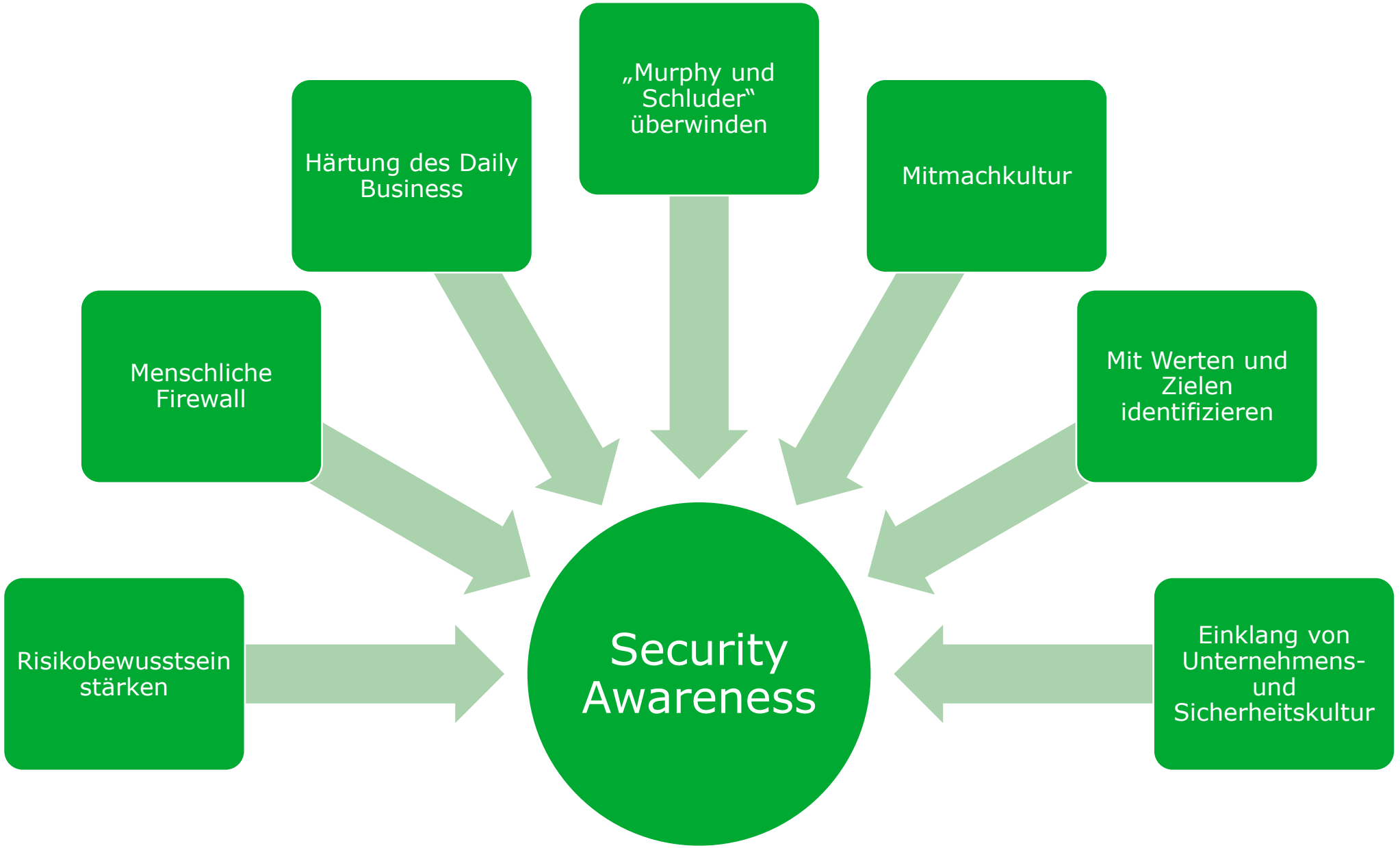
- Identitätsdiebstahl
- Fahrlässiger Informationsabfluss
- Einfallstor für Schadsoftware
- Verminderung der Produktivität
- Social Engineering durch „gefühlte Nähe“

Alles was Sie mit anderen teilen, kann gegen Sie oder Ihre Firma verwendet werden

KONVERTO

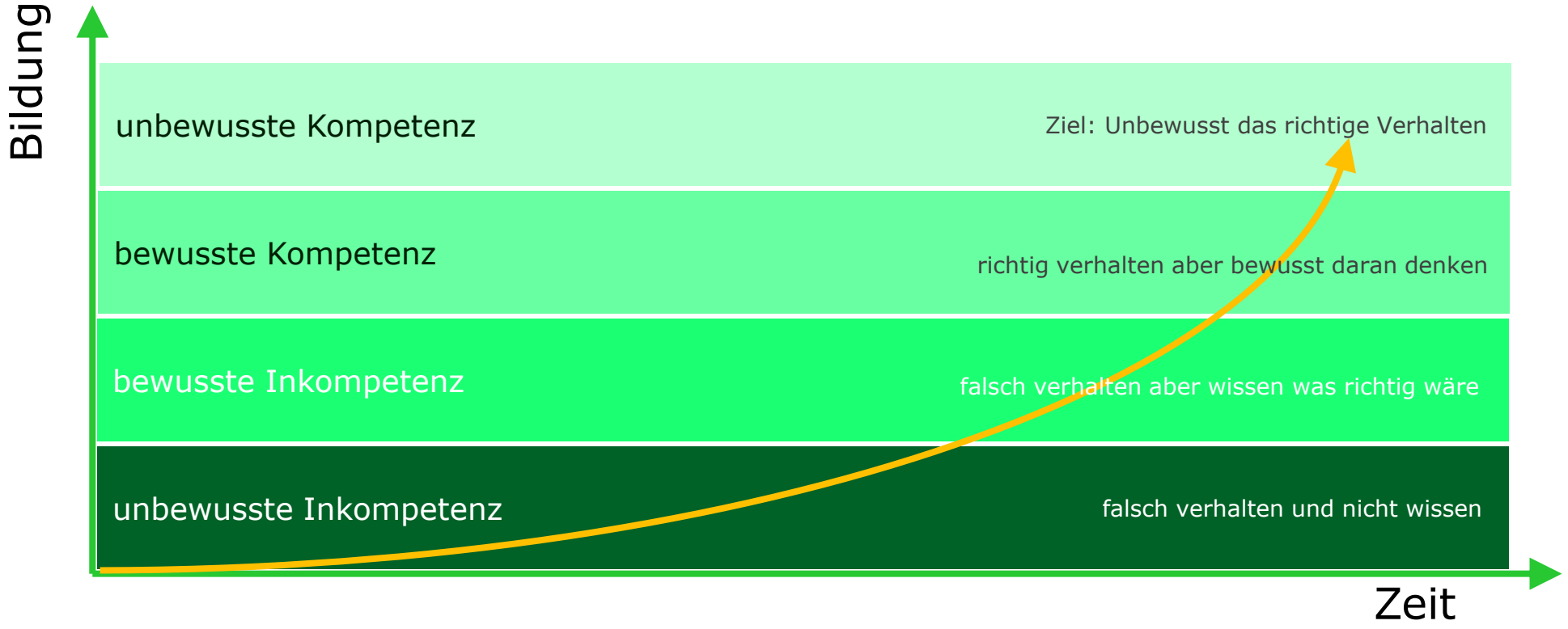
Maßnahmen

KONVERTO


„Murphy und Schluder“ überwinden
Härtung des Daily Business
Mitmachkultur
Menschliche Firewall
Mit Werten und Zielen identifizieren
Risikobewusstsein stärken
Security Awareness
Einklang von Unternehmens- und Sicherheitskultur

KONVERTO

Security Awareness Lernkurve des Menschen



KONVERTO

Security Awareness Themen

Phishing

E-Mail Betrug

Sichere Passwörter

Physische Sicherheit

Sicherheit beim Reisen

Sicherheit in öffentlichen Räumen

Sicheres Surfen

Sicherheit in sozialen Netzwerken

Schutz von mobilen Geräten

Insider Bedrohungen

KONVERTO

Security Awareness Erfolgsfaktoren

- Längerfristig und nachhaltig, Umsetzung in kleinen Schritten
- Alle müssen teilnehmen
- Nicht überfordern, kurze kompakte Einheiten
- Aktive statt passive Teilnahme, praxisrelevante Beispiele, spielerisch, Simulationen
- In der Sprache der Mitarbeiter kommunizieren, nicht technisch
- Privater Nutzen erkennbar
- Guter Mix von Medien

KONVERTO

Die letzte Verteidigungslinie bilden
Sie

Man muss kein hochtechnischer Mensch sein, um ein hochsicherer Mensch zu sein

KONVERTO

passion for technology

Vielen Dank für die Aufmerksamkeit

KONVERTO AG Bruno-Buozzi-Str. 8, Bozen
info@konverto.eu konverto.eu

KONVERTO