HEIDELBERG

LET'S CONNECT

PRINECT ANWENDERTAGE

HEIDELBERG

Sicherheit in der Druckerei:

Erfolgreicher Schutz vor Cyber-Bedrohungen

Disclaimer

Rechtliche Hinweise

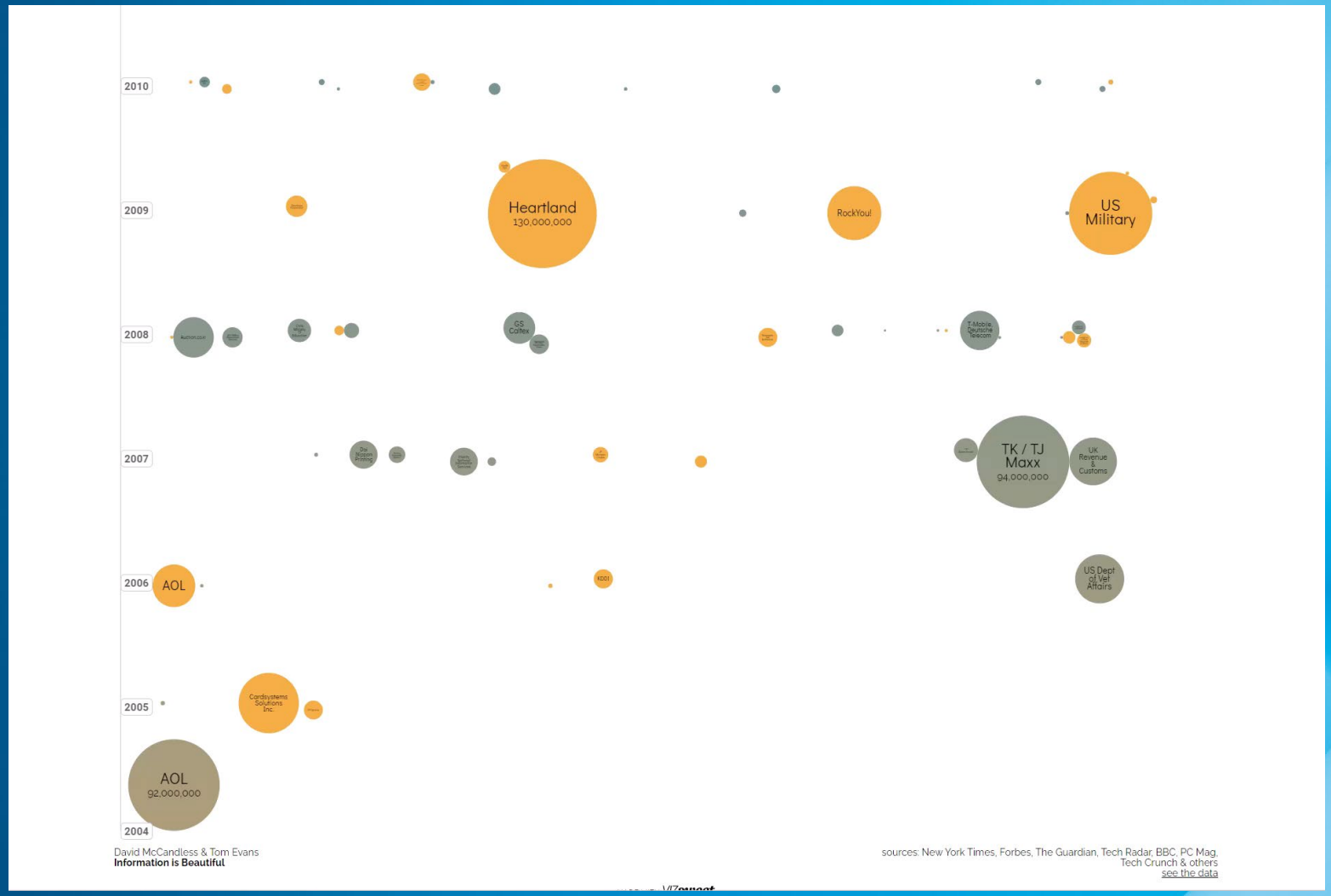
Die Inhalte dieses Workshops wurden mit größter Sorgfalt erstellt. Der Workshop und die darin gegebenen Hinweise ersetzen keinesfalls eine sachkundige, individuelle Beratung durch fachkundige Dritte. Heidelberg übernimmt keine Gewähr für die Richtigkeit, Vollständigkeit und Genauigkeit der Angaben.

Bedrohungs-szenarien

Die größten Angriffstrends

KI-basierte Angriffsmethoden	▪ Deepfakes ▪ Voice Cloning
Phishing und Social-Engineering	▪ Ausspähen sensibler Daten von Opfern
Ransomware	▪ Erpressung nach Datenverschlüsselung
Datendiebstahl	▪ Lösegeld oder Veröffentlichung ihrer Daten
Cyber-Crime-as-a-Service	▪ Der Kriminelle als Kunde der Hack-Branche ▪ standardisierte, käufliche Geschäftsmodelle im Dark Web
Supply-Chain-Attacken	▪ Einschleusen von Malware ▪ Sind Ihre Partner sicherheitstechnisch gut aufgestellt?
Direkte Hackattacken	▪ Der individuelle Hackerangriff
DDoS Angriffe	▪ Systemüberlastung und -lahmlegung ▪ Ihr Geschäft wird blockiert

World's Biggest Data Breaches & Hacks



Quelle: informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Schlussfolgerung:

"Es ist nicht die Frage, ob Sie gehackt werden, sondern wann und wie Sie darauf reagieren."

Mark Minasi

Wie erreicht man ein gutes, eigenes Sicherheitsniveau?

1. Einstellungssache → Sicherheit als Wettbewerbsvorteil betrachten und nicht als unnötige Kosten

2. Widersacher → technische Komplexität und der Faktor Mensch

3. Aktiv werden → Experten involvieren, Best-Practices implementieren und leben

Fragestellungen:

- Was ist für ein gutes, eigenes Sicherheitsniveau nötig?
- Wie kann ich meine Druckerei effektiv gegen Angriffe schützen?
- Welche Sicherheit bietet HEIDELBERG mit seinen Produkten und Dienstleistungen?

Ein gutes eigenes Schutzniveau

Wie erreicht man ein gutes, eigenes Sicherheitsniveau?

Schutzziel der Informationssicherheit:

Vertraulichkeit, **Integrität** und **Verfügbarkeit**
von Informationen sicherstellen

Identifikation der wichtigsten Werte und Informationen sowie deren Schutzbedarf

+

Analyse und Bewertung der Schwachstellen und weißen Flecken auf der Sicherheitslandkarte

⇨ **Risikobewertung**

Wie erreicht man ein gutes, eigenes Sicherheitsniveau?

Ernennung eines Sicherheitsbeauftragten *[Chief (Information) Security Officer (CSO/CISO)]*

- ist treibende Kraft für die Sicherheit in der Druckerei
- eingebunden in Entscheidungsprozesse
- verantwortet Incident Response Team (IRT)

Informationssicherheit ist ein laufender Prozess!

- erfordert kontinuierliche Verbesserung
- Sicherheitsüberprüfungen regelmäßig durchführen
- aktuelle Bedrohungen und Sicherheitstrends im Blick behalten
- Schutzniveau aufrechterhalten und kontinuierlich verbessern

Effektiv gegen Angriffe schützen

Wie kann ich meine Druckerei effektiv gegen Angriffe schützen?

Präventive Maßnahmen

Schulung und Sensibilisierung:

- Mitarbeiter im Umgang mit Sicherheitsrisiken schulen und für die Bedrohung durch Cyber Angriffe sensibilisieren
  - Verstehen der Informationssicherheit
  - Gewährleistung der Datensicherheit sowie des Datenschutzes
  - Gewährleistung der physischen Sicherheit
  - "Best Practices" für sicheres Arbeiten mit dem Computer, einschließlich Remote- und mobilem Arbeiten
  - Was ist zu tun, wenn eine Bedrohung oder ein Verstoß vorliegt?
- Erkennen von Phishing-Angriffen, Social-Engineering-Taktiken, Malware, Datenschutzvorfällen
- sicherer Umgang mit (Druck-)Daten von Kunden/Dritten

Zugriffskontrolle:

- Zugriff auf sensible Daten und Systeme auf autorisierte Benutzer begrenzen
- starke Passwörter, Multi-Faktor-Authentifizierung (MFA), Anbindung des Domänen-Verzeichnisdienst

Software-Update- und Patch-Management:

- alle Systeme und Software auf dem neuesten Stand halten
- regelmäßig Sicherheitsupdates und Patches installieren, um bekannte Schwachstellen zu beheben

Wie kann ich meine Druckerei effektiv gegen Angriffe schützen?

Präventive Maßnahmen

Netzwerksicherheit:

- Netzwerk vor unautorisierten Zugriffen schützen
- Sicherheitsrichtlinien implementieren, um Datenverkehr zu überwachen und zu filtern
- Websysteme absichern (WAF, DMZ, Reverse Proxy etc.)

Physische Sicherheit:

- physischen Zugang zu wichtigen Ressourcen wie Druckmaschinen, Serverräumen und sensiblen Dokumenten schützen

Firewalls und Antivirus-Software:

- Firewalls und Antivirus-Software einsetzen
- Netzwerkverkehr überwachen
- schädliche Aktivitäten erkennen

(Druck-)Datenentgegennahme/-austausch:

- PDFs auf Schadcode prüfen (z.B. Adobe „geschützter Modus“, Öffnen von Kundendaten in „Sandbox“ etc.)
- unsicheres FTP, SMB etc.: File-Sharing-Lösungen abschaffen

Wie kann ich meine Druckerei effektiv gegen Angriffe schützen?

Erkennende Maßnahmen

Sicherheitsüberwachung:

- Überwachung und Analyse des Netzwerkverkehrs implementieren, um verdächtige Aktivitäten zu erkennen
- Intrusion Detection Systems (IDS): Erkennung unautorisierten Zugriffs.
- Sicherheitsrichtlinien und Verfahren: Erstellung von Richtlinien und Verfahren zur Erkennung und Reaktion auf Sicherheitsvorfälle.

Korrigierende Maßnahmen

Incident Response Plan:

- Plan entwickeln, um auf Sicherheitsvorfälle reagieren zu können
- inklusive Erkennung, Reaktion und Wiederherstellung nach einem Cyberangriff

Wiederherstellende Maßnahmen

Datensicherung und Wiederherstellung:

- regelmäßige Backups schutzbedürftiger Daten und Systeme erstellen
- Backups an einem sicheren Ort aufbewahren
- Wiederherstellung (Desaster Recovery) regelmäßig üben

Wie kann ich meine Druckerei effektiv gegen Angriffe schützen?

Abschreckende Maßnahmen

Netzwerksicherheit:

- Netzwerksegmentierung (Office Netz, Drucksaalnetz...), um Risiken durch die Isolierung von Netzwerken zu begrenzen

Organisatorische Maßnahmen

Compliance und Datenschutz:

- Sicherstellen, dass alle relevanten rechtlichen Anforderungen und Datenschutzvorschriften eingehalten werden,
- insbesondere wenn dies sensible Kundeninformationen betrifft
- Einhaltung von Standards (etwa Payment-Standards)

Sicherheitsrichtlinien und -verfahren:

- Entwicklung und Umsetzung von internen Richtlinien und Verfahren zur Gewährleistung der Informationssicherheit

Sicherheit der HEIDELBERG Produkte

Modell der geteilten Verantwortung

ISMS zertifiziert nach ISO/IEC 27001

Shared Responsibility Model

Druckerei

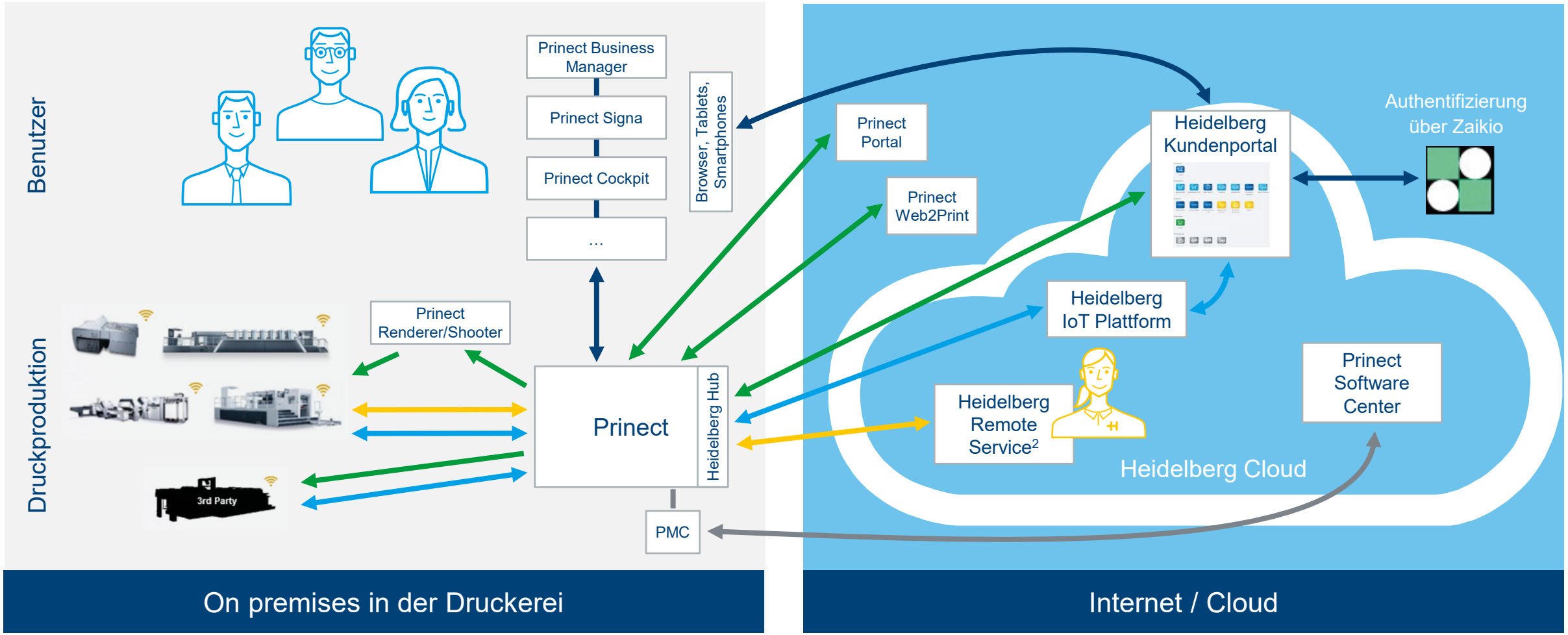
Heidel-berger Druck

Dritte (Cloud Service Provider etc.)

On Premises in der Druckerei	HEIDELBERG Cloud (Software as a Service)
Kundendaten Betriebs- und Produktionsdaten, Druckauftragsdaten, Kundenstammdaten, Materialdaten, Benutzerdaten, Organisationsdaten etc.	
Anwendungsbetriebssicherheit distributierte Software (Prinect, Maschinensoftware etc.)	Anwendungs-/Plattformbetriebssicherheit HEIDELBERG Kundenportal, HEIDELBERG IoT Plattform, Remote Service etc.
Sicherheit der distributierten Software Prinect, DFEs etc.	Sicherheit der Anwendungen/Plattformen HEIDELBERG Kundenportal, HEIDELBERG IoT Plattform, Remote Service etc.
Sicherheit der Maschinen/IoT-Geräte Software Druckmaschinen, Post-Press-Maschinen, CtP-Geräte etc.	Plattformsicherheit
Betriebssystemsicherheit	Betriebssystemsicherheit
Netzwerksicherheit	Netzwerksicherheit
Sicherheit der virtualisierten Infrastruktur	Sicherheit der virtualisierten Infrastruktur
Sicherheit der physikalischen Infrastruktur Hardware, Rechenzentren, Drucksaal, Gebäude etc.	Sicherheit der physikalischen Infrastruktur Hardware, Rechenzentren, Gebäude etc.

HEIDELBERG IT-Sicherheitsarchitektur

Druckereien mit Prinect Workflow[1]



[1] Prinect Production Manager, Prinect Production System, Pressroom Manager, Prepress Manager, Integration Manager; alle mindestens ab Software Version 21.10

[2] sofern Wartungsvertrag besteht

100%ige Sicherheit gibt es nicht

"Das einzige wirklich sichere System ist eines, das ausgeschaltet,
in einen Betonblock gegossen und
in einem mit Blei ausgekleideten Raum
mit bewaffneten Wachen verschlossen ist
– und selbst da habe ich meine Zweifel."

Gene Spafford

Herzlichen Dank für Ihre Aufmerksamkeit!