Praxisszenario

Notfallmanagement für kritische IT-Infrastruktur

Inhalt

Ausgangsszenario

Unternehmensprofil: IndustrieWerk AG

Firmendaten und Geschäftstätigkeit

- **Name:** IndustrieWerk AG - Präzisionsteile für Automotive & Aerospace
- **Gründung:** 1978 (traditionsreiches ostdeutsches Familienunternehmen)
- **Rechtsform:** Aktiengesellschaft (seit 2010)
- **Jahresumsatz:** 85 Millionen € (2024)
- **Mitarbeiter:** 450 (Stammbelegschaft) + 50 Zeitarbeiter
- **Branche:** Tier-1 Automobilzulieferer für BMW, Audi, Mercedes-Benz

Standortverteilung

Hauptsitz Bad Frankenhausen/Kyffhäuser, Thüringen (300 MA):

- Verwaltung und Entwicklungszentrum
- 2 Produktionslinien für Aluminiumgussteile
- Qualitätslabor und Messtechnik
- IT-Rechenzentrum und Serverraum

Werk Leipzig, Sachsen (150 MA):

- 1 Speziallinie für Magnesiumkomponenten
- Oberflächenbehandlung und Beschichtung
- Logistikzentrum für Osteuropa

Kritische Geschäftsabhängigkeiten

Hauptkunden (kritische Abhängigkeiten):

- BMW Group: 35% Umsatzanteil (Motor- und Getriebegehäuse)
- Audi AG: 25% Umsatzanteil (Fahrwerkskomponenten)
- Mercedes-Benz: 20% Umsatzanteil (Strukturbauteile)
- Aerospace-Sektor: 15% (Airbus-Zulieferung über Tier-2)
- Aftermarket: 5% (Ersatzteile)

Supply Chain Risiken:

- **Rohstoffe:** 80% Aluminium aus Norwegen (Hydro ASA)
- **Werkzeuge:** Spezialwerkzeuge aus Italien (6 Monate Lieferzeit)
- **Energie:** 40% des Produktionsstroms aus lokaler Photovoltaik

IT-Infrastruktur & Digitalisierungsgrad

Kernsysteme (alle Windows-basiert)

ERP-System (SAP S/4HANA):

- 15.000 aktive Stammdaten (Artikel, Kunden, Lieferanten)
- 250.000 Buchungssätze/Monat
- Integration mit Produktionsplanung (MES)
- Kundenzugang über SAP Ariba (B2B-Portal)

Produktionssteuerung (SCADA/MES):

- Siemens WinCC für 3 Produktionslinien
- 450 Sensoren und Aktoren vernetzt
- Predictive Maintenance mit KI-Algorithmen
- Quality Gates mit automatischer Fehlererkennung

CAD/PLM-Systeme:

- CATIA V6 für Konstruktion (120 Lizenzen)
- Teamcenter PLM für Produktdatenmanagement
- 8.500 aktive 3D-Modelle und technische Zeichnungen
- Direktanbindung zu Kunden-Systemen (BMW ProE, Audi Matrix)

IT-Sicherheitsarchitektur (vor dem Angriff)

Netzwerk-Topologie:

- **Verwaltungsnetz (VLAN 10):** 180 Client-PCs, 25 Server
- **Produktionsnetz (VLAN 20):** 15 SCADA-Workstations, 8 Industrie-PCs
- **DMZ (VLAN 30):** Web-Server, E-Mail-Gateway, VPN-Konzentrtor
- **Management-VLAN (VLAN 99):** Switches, Firewalls, Monitoring

Sicherheitsmaßnahmen (unzureichend):

- Palo Alto Firewall (ungepatchte Version PA-OS 9.1)
- Windows Defender auf allen Clients (zentral verwaltet)
- Backup-System: Veeam auf Synology NAS (täglich, 30 Tage Retention)
- VPN-Zugang: Cisco AnyConnect (ohne MFA!)
- Patch-Management: manuell, alle 3 Monate

Compliance & Regulatorische Anforderungen

Automotive-Zertifizierungen:

- ISO 9001:2015 (Qualitätsmanagement)
- IATF 16949:2016 (Automotive Quality)
- ISO 14001:2015 (Umweltmanagement)
- **TISAX-Zertifizierung:** geplant für Q2/2025

DSGVO-Compliance:

- 15.000 Mitarbeiterdatensätze
- 8.500 B2B-Kundendaten (Verträge, Preislisten)
- Datenschutzbeauftragte (extern): Kanzlei Weber & Partner
- **Schwachstelle:** Keine Verschlüsselung der HR-Datenbank

Kritische Infrastruktur-Relevanz:

- **Kein KRITIS-Betreiber** nach BSI-KritisV (unter Schwellenwerten)[3][4]
- Aber: **Systemrelevant für BMW-Produktion** (Just-in-Time Lieferung)
- **Einzelausfallrisiko:** Bestimmte Bauteile nur bei IndustrieWerk verfügbar

Marktposition & Wettbewerbsumfeld

Marktstellung

- **Regional:** Nr. 2 Automobilzulieferer in Thüringen (nach Bosch)[2][1]
- **Technologie:** Spezialist für Leichtbau und Hybridmaterialien
- **Innovation:** 5% Umsatz in F&E (Elektromobilität-Transformation)
- **Abhängigkeit:** 80% Umsatz aus Verbrenner-Komponenten (Transformationsrisiko)

Strategische Herausforderungen 2025

Branchentrends und Druck:[5][1]

- **Elektrifizierung:** Wegfall traditioneller Motorkomponenten
- **Kostendruck:** OEMs fordern jährlich 3-5% Preisreduktion
- **Lieferkettenrisiken:** Abhängigkeit von China/Taiwan (Rohstoffe)
- **Fachkräftemangel:** 25 offene Stellen (Ingenieure, IT-Spezialisten)

Konkurrenzsituation

Direkte Wettbewerber:

- **Bohai Trimet Automotive** (Sömmerda): Hauptkonkurrent
- **Borbet Thüringen** (Bad Langensalza): Leichtmetallräder
- **Magna** (Baunatal): Globaler Riese mit Preis-/Skalenvorteil

Cyber-Bedrohungslandschaft Automotive:[6][5]

- 30% aller Ransomware-Angriffe treffen Fertigungsindustrie
- Deutschland Platz 3 weltweit bei Ransomware-Opfern
- Besonders gefährdet: KMU ohne eigene IT-Security-Teams
- Häufigste Angreifer: LockBit 3.0, BlackBasta, RansomHub

Organisationsstruktur & Schlüsselpersonen

Vorstand & Geschäftsführung

- **CEO:** Dr. Marcus Schneider (58), seit 2015, Ex-BMW Manager
- **CTO:** Dr. Sarah Weber (45), seit 2018, Maschinenbau TU Dresden
- **CFO:** Klaus Hartmann (52), seit 2020, Ex-Wirtschaftsprüfer

Betriebsrat & Mitarbeiterwesen

- **Betriebsratsvorsitzender:** Thomas Fischer (IG Metall, 15 Jahre im Unternehmen)
- **Belegschaftsstruktur:** 40% über 50 Jahre, 25% unter 35 Jahre
- **Qualifikationen:** 60% Facharbeiter, 25% Ingenieure/Techniker, 15% Verwaltung

IT-Organisation (Schwachstelle!)

- **IT-Leiter:** Michael Weber (43), Autodidakt, seit 10 Jahren im Unternehmen
- **IT-Team:** 4 Administratoren (2x Windows, 1x Netzwerk, 1x SAP)
- **Externes:** Wartungsverträge mit 3 verschiedenen Dienstleistern
- **Kein ISMS vorhanden,** keine formellen Security-Prozesse
- **Letztes Security-Audit:** 2019 (für ISO 9001)

Gefahrenszenario-Kontext: Warum gerade IndustrieWerk?

Attraktivitätsfaktoren für Cyberkriminelle

Hohe Zahlungsbereitschaft:

- **Just-in-Time Produktion:** Jede Stunde Stillstand = 25.000€ Verlust
- **Reputationsrisiko:** BMW/Audi-Lieferausfall = existenziell
- **Versicherungsschutz:** 5 Mio. € Cyber-Police signalisiert Zahlungsfähigkeit

Schwache Cyber-Abwehr:

- **Veraltete Systeme:** Windows Server 2016 ohne aktuelle Patches
- **Fehlende MFA:** VPN-Zugang nur mit Username/Passwort
- **Unzureichende Segmentierung:** Verwaltung + Produktion im selben Netz
- **Backup-Schwachstelle:** Tägliche Backups, aber nicht offline/immutable

Industriespionage-Potenzial:

- **BMW iNext Projekte:** Vertrauliche Konstruktionsdaten im PLM-System
- **Konkurrenzrelevante Daten:** Kalkulationen, Kundenlisten, Technologien
- **Supply Chain Access:** Sprungbrett zu BMW/Audi-Systemen möglich

Der perfekte Sturm - September 2025

Verschärfende Umstände:

- **Urlaubszeit:** 30% IT-Personal im Urlaub (Sommerloch)
- **Projektdruck:** BMW iNext Serienstarts in 4 Wochen
- **Corona-Nachwirkungen:** Viele Mitarbeiter noch im Homeoffice
- **Investitionsstau:** IT-Budget seit 2020 eingefroren

Angriffsfenster:

- **Freitagabend-Angriff:** Minimale IT-Besetzung am Wochenende
- **Ferienzeit:** Externe Dienstleister schwer erreichbar
- **Montagsproduktion:** Maximaler Druck für schnelle Entscheidungen

Das Gefahrenszenario im Detail

Erste Phase: Angriffserkennung (08:15 - 08:45 Uhr)

Ein Mitarbeiter der Frühschicht meldet dem IT-Support, dass die Produktionssteuerung (SCADA-System) nicht mehr reagiert und verschlüsselte Dateien auf mehreren Servern anzeigt. Gleichzeitig fallen E-Mail-Server und ERP-System aus. Eine Ransomware-Nachricht fordert 1,5 Millionen Euro Lösegeld binnen 72 Stunden.

Betroffene Systeme:

- Produktionssteuerung (SCADA/MES-Systeme)
- ERP-System (SAP) mit Kundendaten und Auftragsmanagement
- E-Mail- und Groupware-Server
- Backup-Systeme (teilweise kompromittiert)
- Netzwerk-Infrastruktur zwischen Produktion und Verwaltung

Sofortige Auswirkungen:

- 3 Produktionslinien stehen still (Verlust: 25.000€/Stunde)
- 200 Mitarbeiter können nicht arbeiten
- Kommunikation mit Kunden und Lieferanten unterbrochen
- Liefertermine für wichtige Aufträge gefährdet

Mögliche Lösungsstrategie nach IT-Grundschutz

1. Sofortmaßnahmen (0-2 Stunden)

Krisenteam aktivieren:

- Notfallbeauftragte/r übernimmt Leitung
- IT-Sicherheitsbeauftragte/r koordiniert technische Maßnahmen
- Geschäftsführung für strategische Entscheidungen einbeziehen
- Externe Forensik-Experten kontaktieren

Containment-Maßnahmen:

- Isolierung betroffener Netzwerksegmente
- Shutdown kritischer Systeme zur Schadensbegrenzung
- Sicherung forensischer Evidenz vor weiteren Maßnahmen
- Aktivierung des Incident Response Plans gemäß DER.2.1[1]

2. Bewertung und Analyse (2-8 Stunden)

Business Impact Assessment:

- Kritische Geschäftsprozesse identifizieren (RTO/RPO-Analyse)
- Finanzielle Ausfallkosten quantifizieren
- Compliance-Risiken bewerten (DSGVO-Meldepflicht)
- Alternative Produktionsmöglichkeiten prüfen

Technische Analyse:

- Backup-Integrität prüfen (letzte saubere Sicherung)
- Angriffsvektor und -umfang ermitteln
- Forensische Untersuchung einleiten
- Recovery-Strategien entwickeln

3. Kommunikationsstrategie

Interne Kommunikation:

- Mitarbeiter über alternative Arbeitsplätze/Prozesse informieren
- Betriebsrat und Führungskräfte briefen
- Regelmäßige Updates im 2-Stunden-Takt

Externe Kommunikation:

- Kunden über Lieferverzögerungen informieren
- Lieferanten über geänderte Abläufe benachrichtigen
- Datenschutzbehörde binnen 72h informieren
- Versicherung und Rechtsberatung einschalten

4. Recovery-Phase (8-72 Stunden)

Technische Wiederherstellung:

- Neuaufbau kritischer Systeme aus sauberen Backups
- Implementierung zusätzlicher Sicherheitsmaßnahmen
- Stufenweise Wiederinbetriebnahme nach Priorität
- Kontinuierliche Überwachung auf weitere Angriffe

Geschäftsprozess-Recovery:

- Manuelle Ersatzverfahren für kritische Prozesse
- Temporäre Auslagerung von Produktionskapazitäten
- Nachholung von Aufträgen nach Priorität
- Kundenkommunikation über Wiederaufnahme

Präventive Maßnahmen (Lessons Learned)

Technische Verbesserungen:

- Implementierung von Mikrosegmentierung im Netzwerk
- Verbesserung der Backup-Strategien (3-2-1-Regel mit Offline-Kopien)
- Installation von EDR/XDR-Lösungen für bessere Erkennung
- Härtung kritischer Systeme nach IT-Grundschutz-Bausteinen

Organisatorische Maßnahmen:

- Regelmäßige Notfallübungen mit verschiedenen Szenarien
- Schulung aller Mitarbeiter zu Cyber-Bedrohungen
- Überarbeitung des Notfallhandbuchs
- Aufbau redundanter Kommunikationswege

Strategische Entscheidungen:

- Cyber-Versicherung mit erweiterten Deckungssummen
- Aufbau eines SOC (Security Operations Center)
- Externe Incident Response-Verträge abschließen
- Regelmäßige Penetrationstests und Schwachstellenanalysen

Erfolgsmessung und Validierung

Kennzahlen für Recovery:

- RTO erreicht: Produktionswiederaufnahme binnen 48h
- RPO minimal: Datenverlust unter 4 Stunden
- Kommunikationsziele: 95% Stakeholder binnen 6h informiert
- Finanzielle Schäden: Unter 500.000€ durch schnelle Response

Kontinuierliche Verbesserung:

- Quarterly Reviews des Notfallmanagements
- Update der Business Continuity Pläne
- Integration neuer Bedrohungslagen
- Anpassung an regulatorische Änderungen

Dieses Szenario zeigt, wie systematisches Notfallmanagement nach IT-Grundschutz-Prinzipien auch bei schwerwiegenden Cyberangriffen strukturierte Recovery-Prozesse ermöglicht und sowohl Schäden minimiert als auch organisationales Lernen fördert.