ausecus.
Automation Security Services GmbH

Industrial IT Security

Konkrete Lösungsansätze am Beispiel der Lebensmittelindustrie

Wir sorgen für die Sicherheit Ihrer Anlagen

eco-Verband Frankfurt, 18.06.2013
Kent Andersson

eco

Industrial IT Security.

1. Aktualität und Realität

2. Häufige Sicherheitsprobleme

3. Konkrete Lösungsansätze

4. Empfehlungen und Zusammenfassung

1. Aktualität und Realität
Aktuelle Medienmeldungen

Quellen: ZDF heute_Journal http://www.zdf.de/ Bayerischen Fernsehen BR3 http://www.br-online.de/

1. Aktualität und Realität

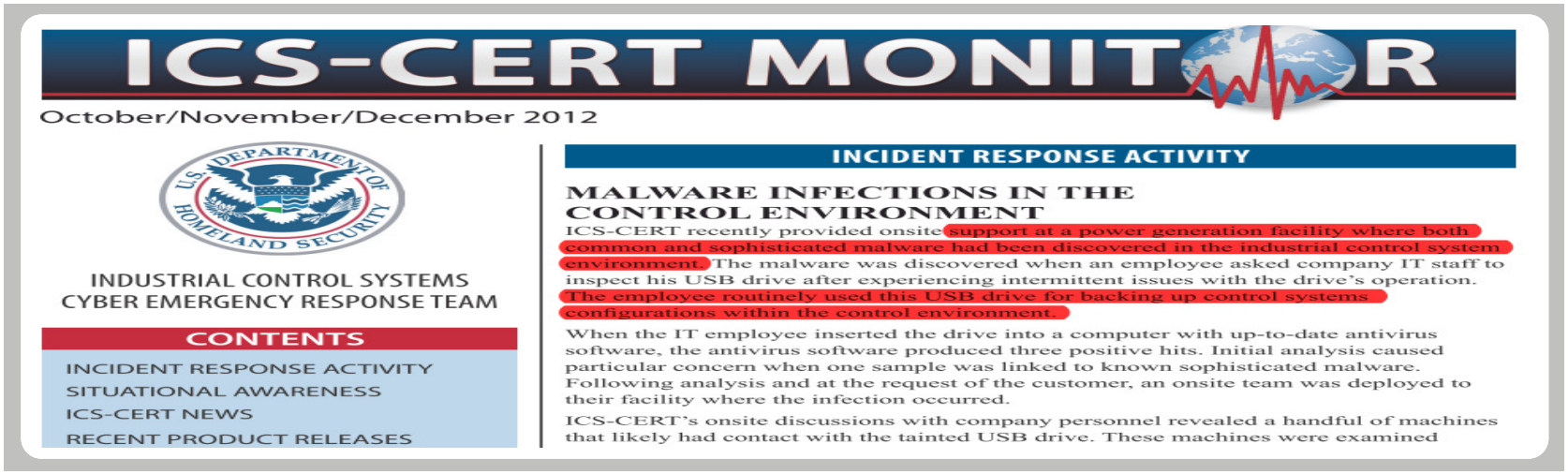
Angriffe auf zwei Stromversorger in Oktober 2012

heise online > News > 2013 > KW 3 > ICS-CERT berichtet von Viren-Infektionen bei US-Stromversorgern

14.01.2013 00:30

ICS-CERT berichtet von Viren-Infektionen bei US-Stromversorgern

Das US-amerikanische Computer Emergency Response Team (**US-CERT** [http://en.wikipedia.org/wiki/United_States_Computer_Emergency_Readiness_Team]) berichtet in seinem aktuellen **ICS-CERT Monitor** [http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_Oct-Dec2012.pdf] von gleich zwei Viren-Infektionen bei US-amerikanischen Stromversorgern im letzten Quartal 2012. In beiden Fällen wurden industrielle Steuerungsanlagen über USB-Sticks infiziert. Die Schädlinge verursachten unter anderem den mehrwöchigen Ausfall eines Elektrizitätswerks.



ICS-CERT MONITOR

October/November/December 2012

INDUSTRIAL CONTROL SYSTEMS
CYBER EMERGENCY RESPONSE TEAM

CONTENTS

INCIDENT RESPONSE ACTIVITY
SITUATIONAL AWARENESS
ICS-CERT NEWS
RECENT PRODUCT RELEASES

INCIDENT RESPONSE ACTIVITY

MALWARE INFECTIONS IN THE CONTROL ENVIRONMENT

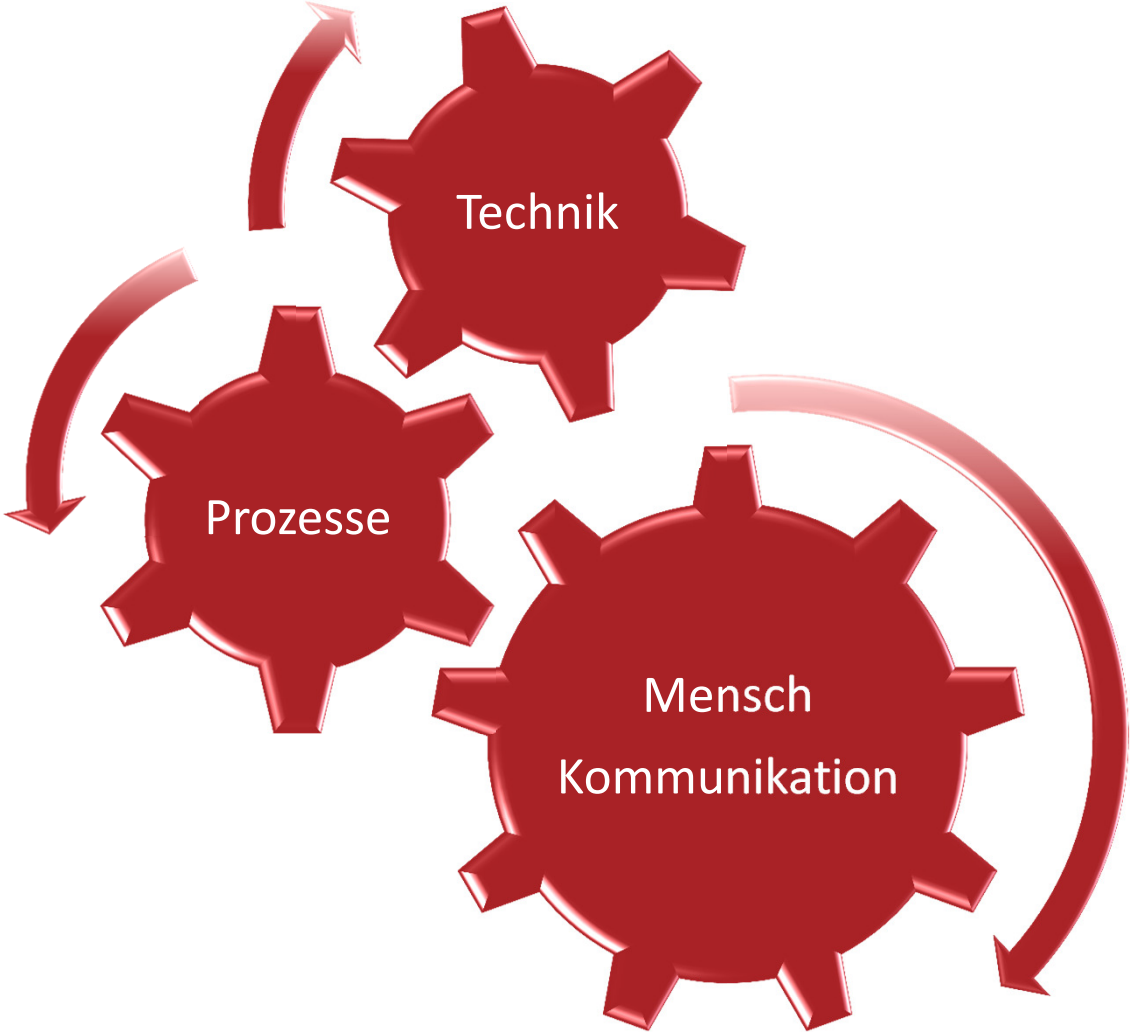
ICS-CERT recently provided onsite support at a power generation facility where both common and sophisticated malware had been discovered in the industrial control system environment. The malware was discovered when an employee asked company IT staff to inspect his USB drive after experiencing intermittent issues with the drive's operation. The employee routinely used this USB drive for backing up control systems configurations within the control environment.

When the IT employee inserted the drive into a computer with up-to-date antivirus software, the antivirus software produced three positive hits. Initial analysis caused particular concern when one sample was linked to known sophisticated malware. Following analysis and at the request of the customer, an onsite team was deployed to their facility where the infection occurred.

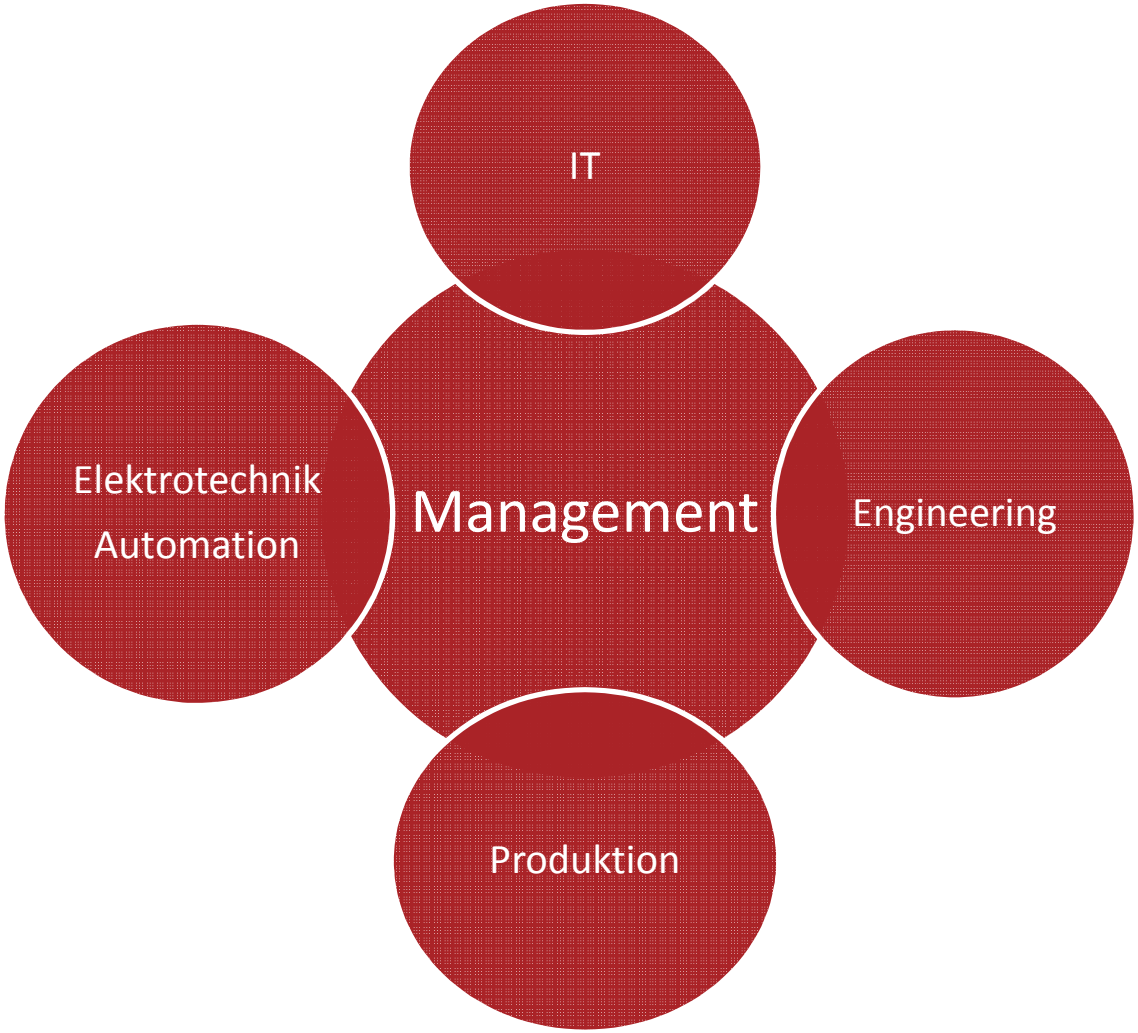
ICS-CERT's onsite discussions with company personnel revealed a handful of machines that likely had contact with the tainted USB drive. These machines were examined

Quellen: heise Security http://www.heise.de/security/ ICS_CERT https://ics-cert.us-cert.gov/

2. Häufige Sicherheitsprobleme
Kompetenzmix

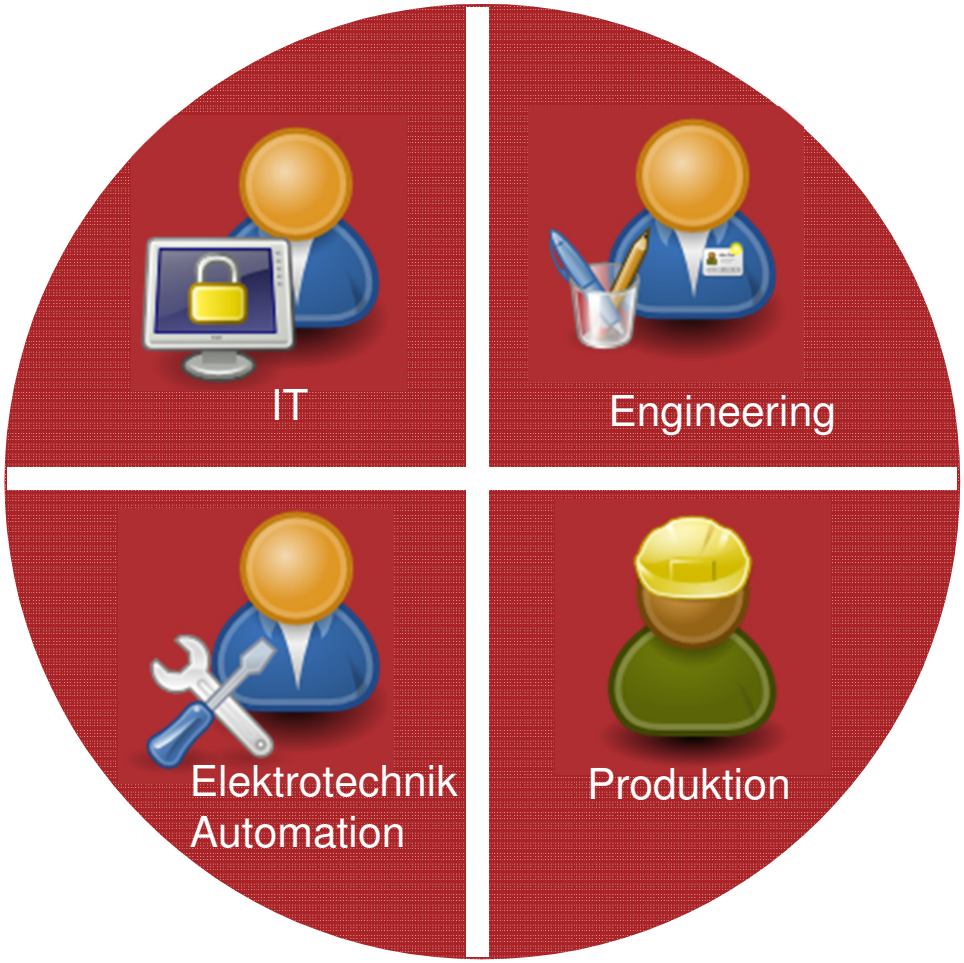


2. Häufige Sicherheitsprobleme
Kompetenzprobleme



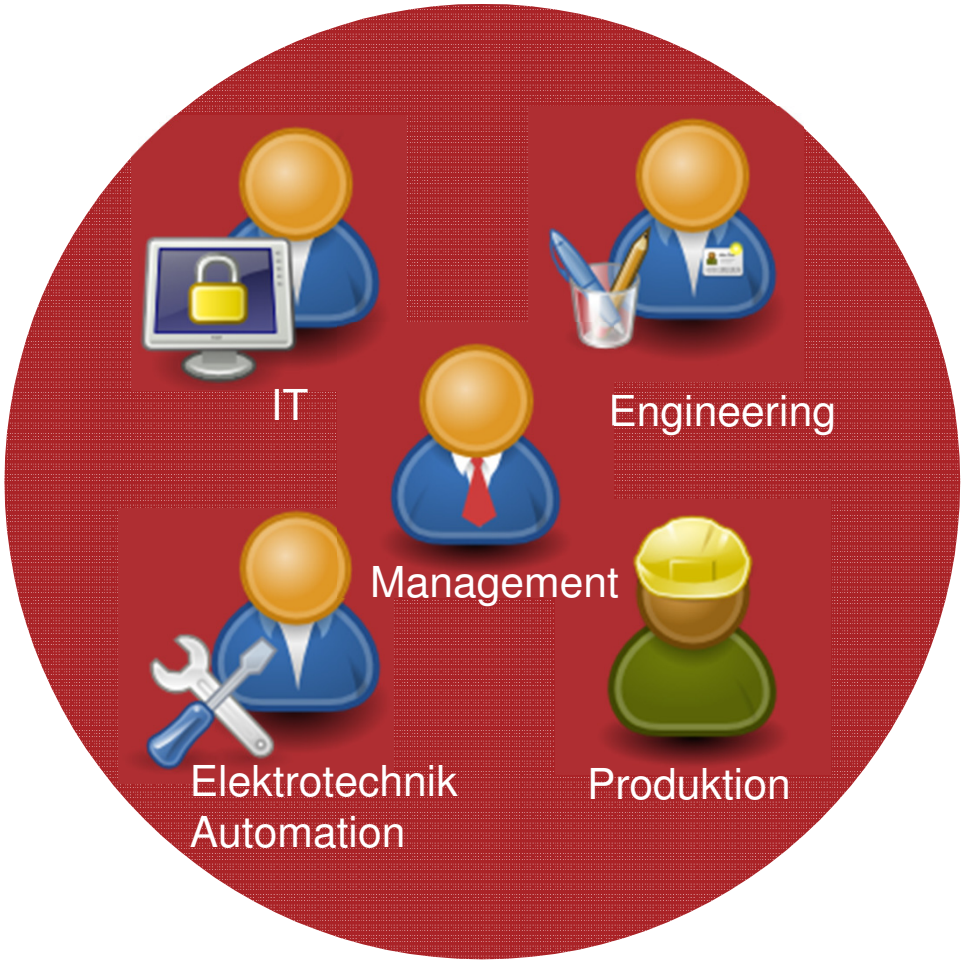
2. Häufige Sicherheitsprobleme
Kompetenzprobleme

Management



Bildquelle: OSA Icon Library http://www.opensecurityarchitecture.org/cms/en/library/icon-library

2. Häufige Sicherheitsprobleme
Zusammenarbeit ist entscheidend für den Erfolg



Bildquelle: OSA Icon Library http://www.opensecurityarchitecture.org/cms/en/library/icon-library

2. Häufige Sicherheitsprobleme
Notebooks

Beispiel: externer Servicetechniker Herr Virusbringer

- Sehr kompetenter, freundlicher Mitarbeiter, 10 Jahre im Betrieb
- Herr V. bringt aber heute etwas herein was keiner will
- Im aktuellen Monat bereits bei 19 Firmen tätig gewesen
- Seit Jahresbeginn in 140 verschiedenen Netzwerken unterwegs
- Auch im firmeneigenen Netzwerk, Zuhause und am Flughafen
- Herr V. hat 30 Kollegen/innen in der Abt. Service
- Über 4.000 Produktions-Netzwerke in diesem Jahr

Mehr als 30.000 neue Viren jeden Tag
Alle 3 Sekunden ein neuer Virus

2. Häufige Sicherheitsprobleme - Notebooks
Lösungsansatz

- Keine fremden Notebooks im Produktionsnetzwerk zulassen
- Firmeneigene Notebooks für externe Servicetechniker bereitstellen

2. Häufige Sicherheitsprobleme
USB-Medien

USB-Schnittstellen und USB-Wechselspeichermedien

- Keine Verwaltung von USB-Medien im Betrieb
- USB-Schnittstellen an den meisten Rechnern offen
- Eigene & externe Mitarbeiter können USB uneingeschränkt nutzen

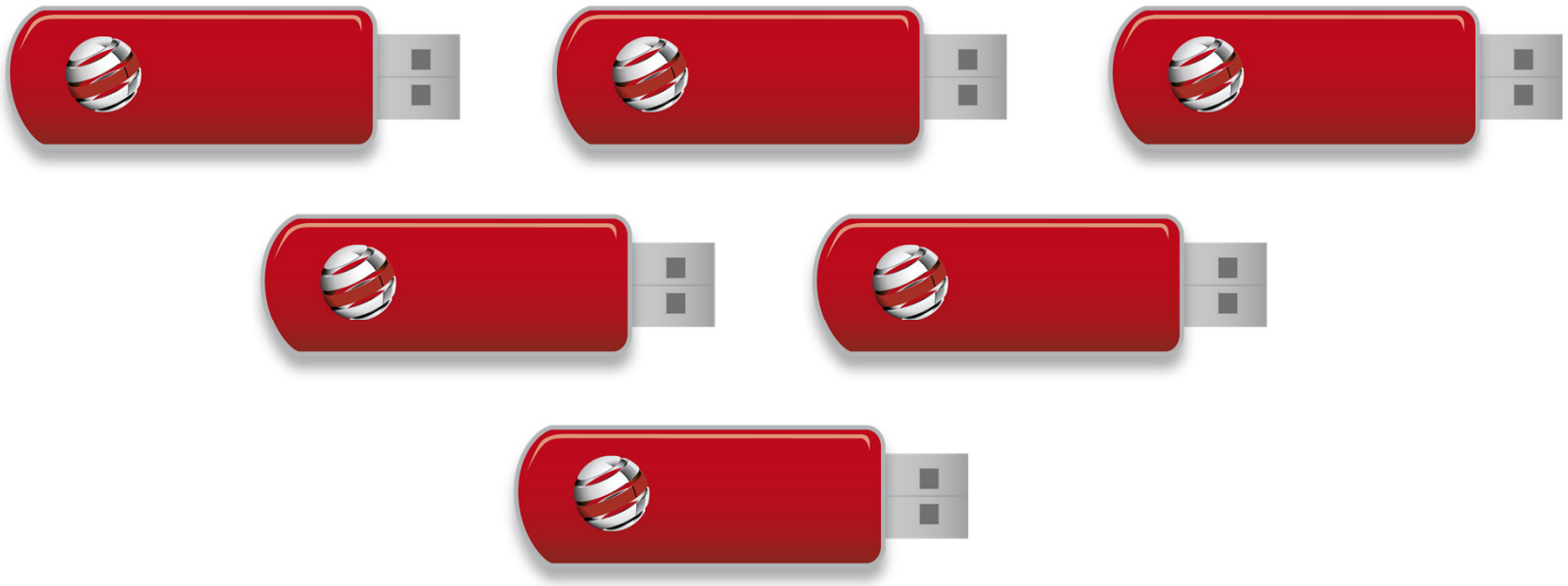
→ Produktionsdaten, Rezepte, Protokolle und Datenbanken kopieren

→ Datendiebstahl und Virusgefahr

USB-Medien sind eine oft unterschätzte Gefahr
Produktionsstillstand als Folge

2. Häufige Sicherheitsprobleme - USB-Medien
Lösungsansatz

- Verwaltung von USB-Medien im Betrieb
- Richtlinie für den Umgang mit USB-Medien einführen
- USB-Schnittstellen kontrolliert absperren



2. Häufige Sicherheitsprobleme
Offene Schnittstellen

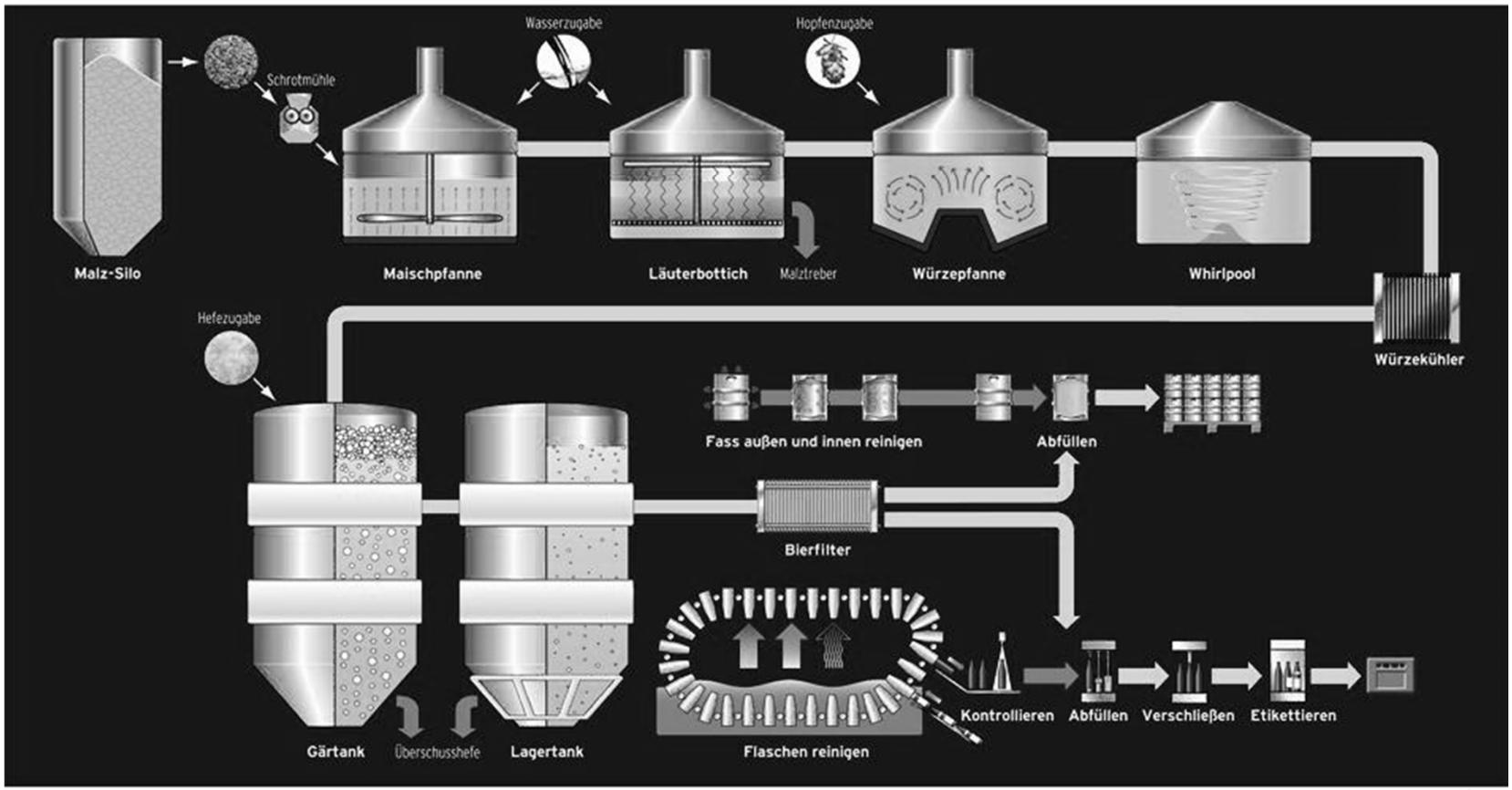
- Vernetzung zwischen Produktions-Netzwerken und Office-IT
- Verbindungen zum Internet
- Fernwartungszugänge
- Offene Kommunikationsports in den Systemen
- Offene USB-Schnittstellen

In 2012 wurden im Projekt SHINE (Shodan Intelligence Extraction) 7.200 offene Visualisierungssysteme in USA im www. gefunden!!!

2. Häufige Sicherheitsprobleme - Offene Schnittstellen
Lösungsansatz

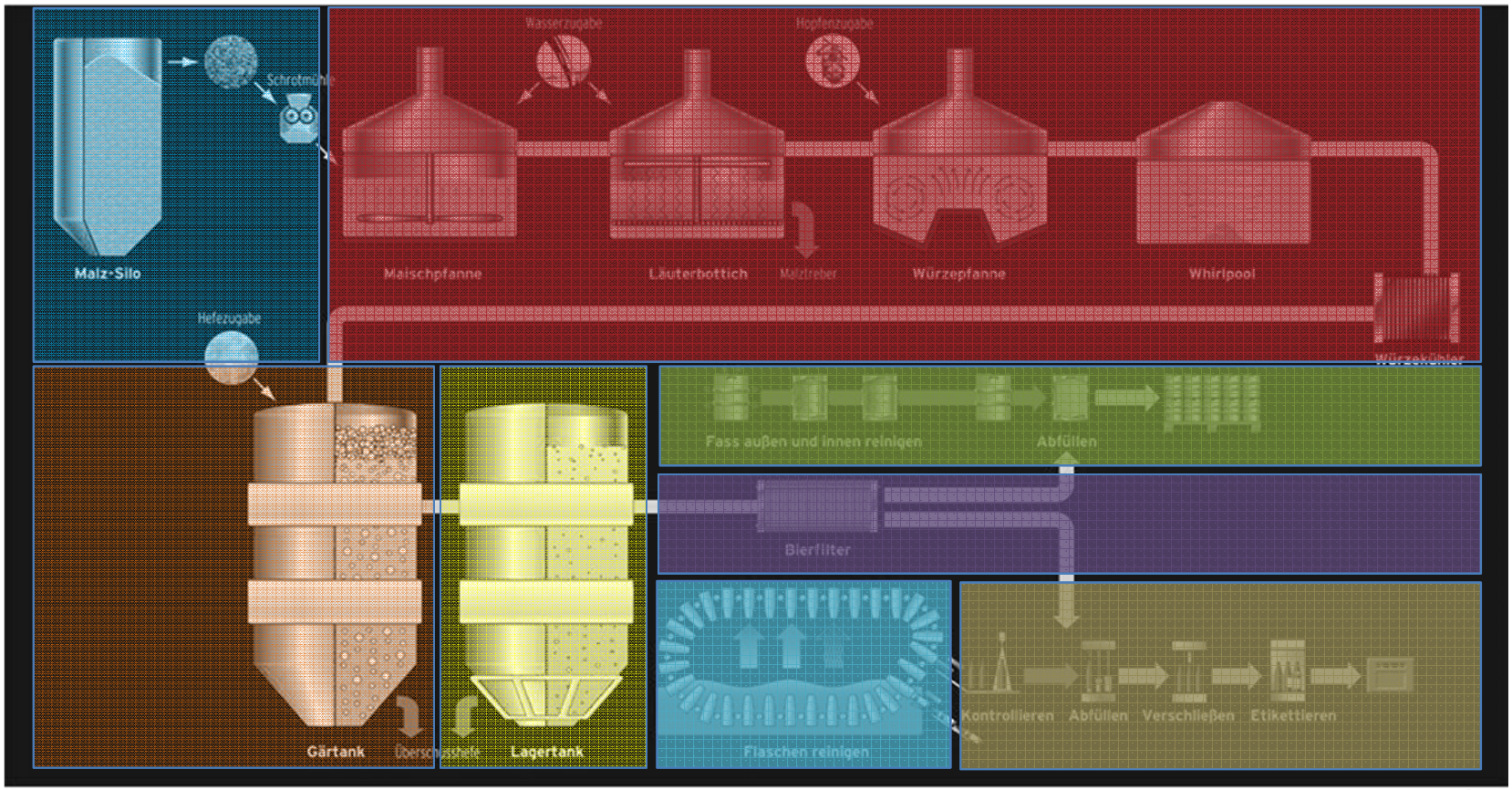
- Produktions-Netzwerke „abschotten“
- Zellenschutz-Konzept
- Firewalls Hutschienenmontage einbauen
- Fernwartungszugänge absichern
- Offene Kommunikationsports aufspüren und zumachen

2. Häufige Sicherheitsprobleme – Referenzkunde
Brauerei



Bildquelle: Deutscher Brauer-Bund e.V. http://www.brauer-bund.de

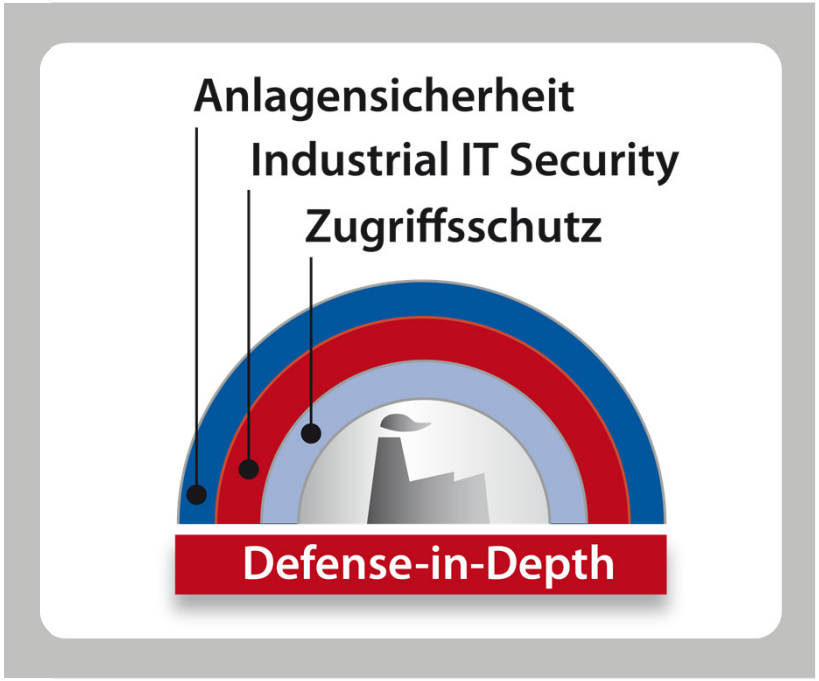
2. Lösung mit Zellenschutz
Brauerei



Bildquelle: Deutscher Brauer-Bund e.V. http://www.brauer-bund.de

3. Konkrete Lösungsansätze
Was ist zu tun?

- 1. Anlagen schützen
  - Physikalischer Zugangsschutz
  - Zutrittskontrolle und abgesperrte Server-und Schaltschränke
- 2. Systeme härten
  - Zellenschutz-Konzept
  - Produktions-Netzwerke „abschotten“
  - Verwaltung USB-Medien und Notebooks
  - USB-Schnittstellen kontrolliert absperren
  - Kommunikation überwachen
  - Whitelisting



Verfügbare Standardprodukte
Bewährte Sicherheitskonzepte
Praktikable Lösungen

3. Konkrete Lösungsansätze
Was ist zu tun?

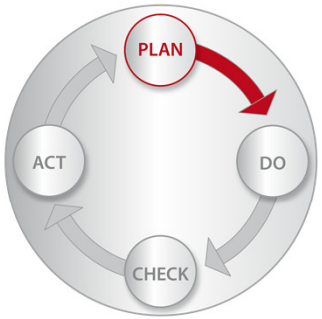
- 3. Menschen
  - Mitarbeiter/innen schulen
  - Bewusstsein schaffen
- 4. Prozesse und Abläufe
  - Abläufe und Richtlinien überprüfen
  - Im QM und im kontinuierlichen Verbesserungsprozess integrieren
  - Verfügbare Standards nutzen
- 5. Vorhandene Normen und Standards nutzen

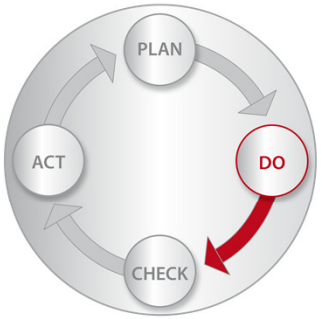
Überschaubarer Aufwand
Kurze Realisierungszeit

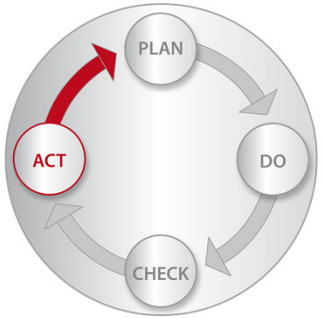
4. Empfehlungen
Konkrete Herangehensweise

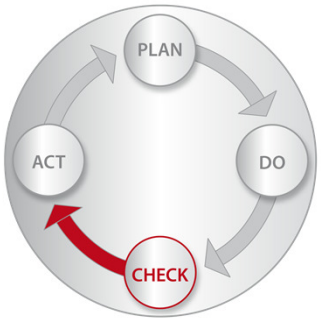
4. Empfehlungen

Security im kontinuierlichen Verbesserungsprozess









ITSECURITY
Member of the Bavarian IT Security & Safety Cluster

eco

ausecus.
Automation Security Services GmbH

Vielen Dank für Ihre Aufmerksamkeit.

Ihr Ansprechpartner: Kent Andersson

Industrial IT Security.
www.ausecus.com