SPECIAL STEEL FOR THE WORLD´S TOP PERFORMERS

Sicherheit 4.0

寶貝進財

Sicherheit

- Der Begriff beschreibt den Zustand „frei von nicht vertretbaren Risiken oder Gefahren“
- Sicherheit in der Technik: Schutz der Arbeitnehmer und Anlagen vor den Gefahren durch
  - Elektrischen Strom
  - Hitze
  - Schmutz
  - Mechanisch bewegten Teilen
  - …

SAFETY

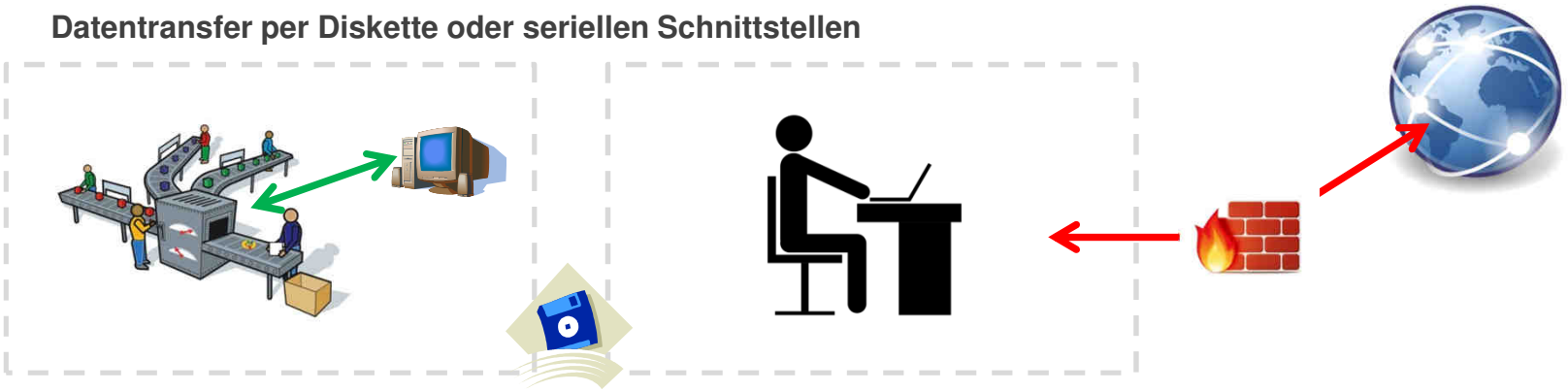
Sicherheit

- Sicherheit in der IT-Umgebung: Schutz der EDV-Systeme vor
  - Unbefugten Zugriffen
  - Unerlaubter Manipulation von Daten
  - Viren
  - Schadsoftware aller Art
  - …

SECURITY

Safety & Security

- Klassische Produktionsmaschinen waren in der Vergangenheit aus IT-Sicht eine „Insel“
- Keine Vernetzung mit der Office-Welt oder dem Internet
- Datentransfer per Diskette oder seriellen Schnittstellen



Safety & Security

- Produktionsanlagen werden durch die fortschreitende Digitalisierung vernetzt
- Durch die Vernetzung erstrecken sich bekannte Gefahren aus der IT-Welt in die Produktionsumgebung
- Die Anwendung von Cloud-basierten Diensten bringt zusätzliche Herausforderungen

(Mindest) Schutz in der Office-IT

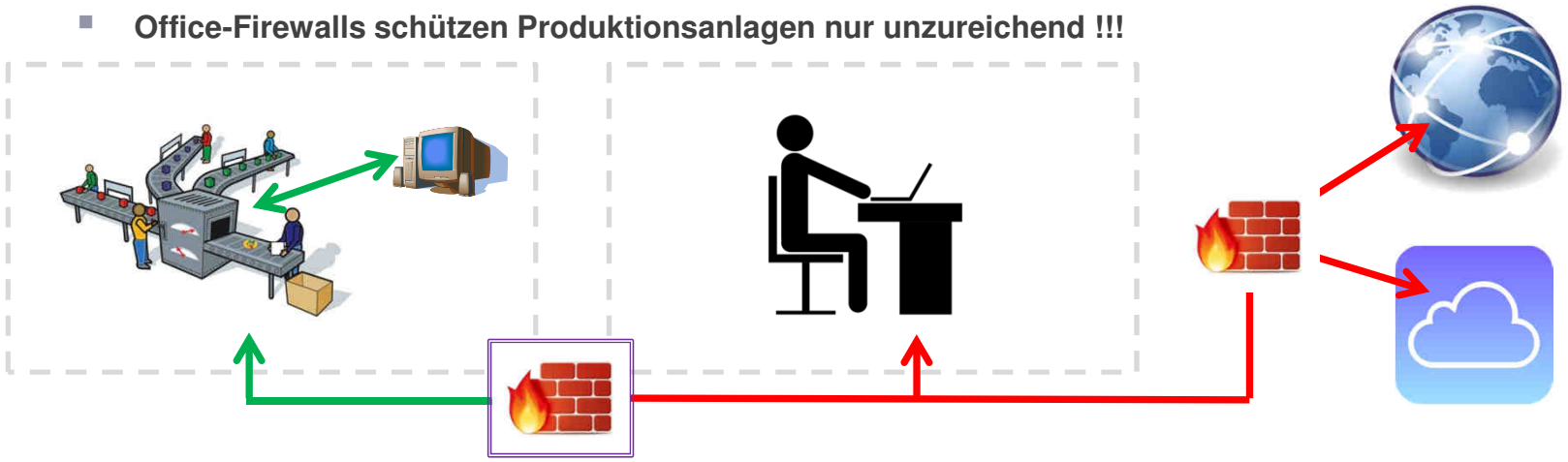
- **Mindest-Schutzmethoden in der klassischen Office-IT**
  - **Virenschutz und Schutz gegen andere Schadsoftware**
  - **Regelmäßige Updates zum Schließen bekannter Sicherheitslücken**
  - **Einsatz von Firewalls innerhalb von Netzwerken und zum Internet**
  - **Zugriffsregelung durch Passwörter oder andere Authentifizierungsmethoden**

Office vs. Produktion

- Schutzmethoden der klassischen Office-IT sind in der Produktion oft nicht anwendbar
- Komponenten von Produktionsanlagen bzw. Steuerungs- und Automatisierungsgeräte bzw. CNC-Steuerungen wurden meist nicht für die Einbindung in „offene“ Netzwerke ausgelegt
  - Sicherheitsupdates sind oft nicht möglich
  - Installation eines Virenschutzes ist nicht möglich
  - Zugriffsschutz durch Passwörter ist oft nicht oder nur unzureichend gegeben
  - Eigenständiger Schutz vor Netzwerkzugriffen ist meist unzureichend oder nicht vorhanden
  - „veraltete“ Betriebssysteme im Einsatz

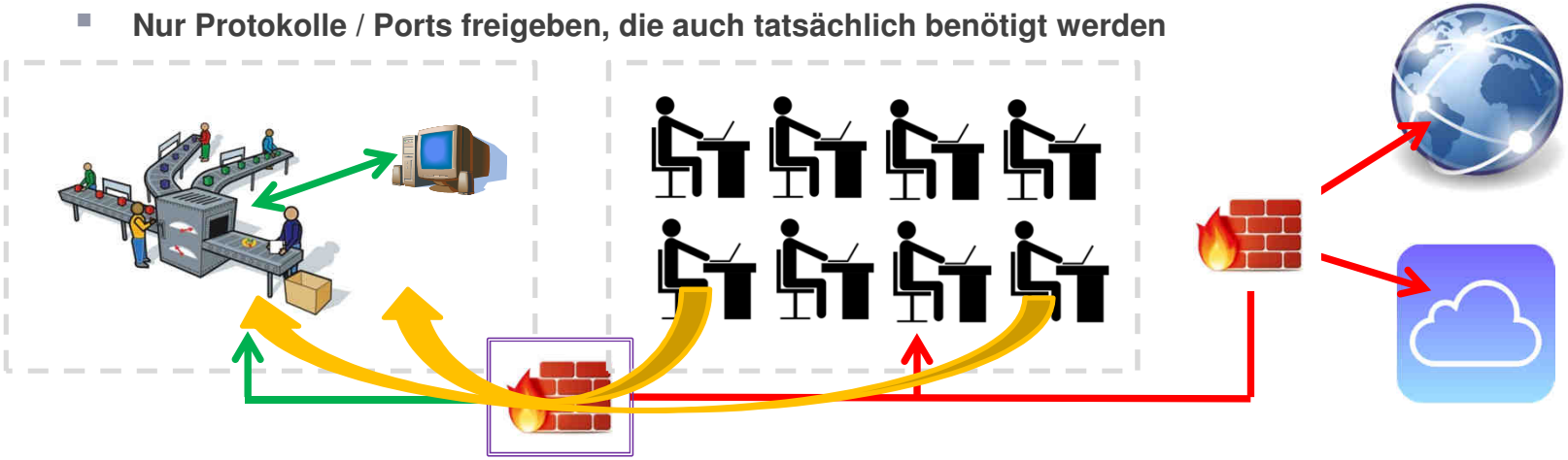
Schutz für Produktionsanlagen

- Aufteilung / Segmentierung der Netzwerke (Office und Produktion)
  - Einsatz von geeigneten Firewalls zwischen den Bereichen
  - Office-Firewalls schützen Produktionsanlagen nur unzureichend !!!



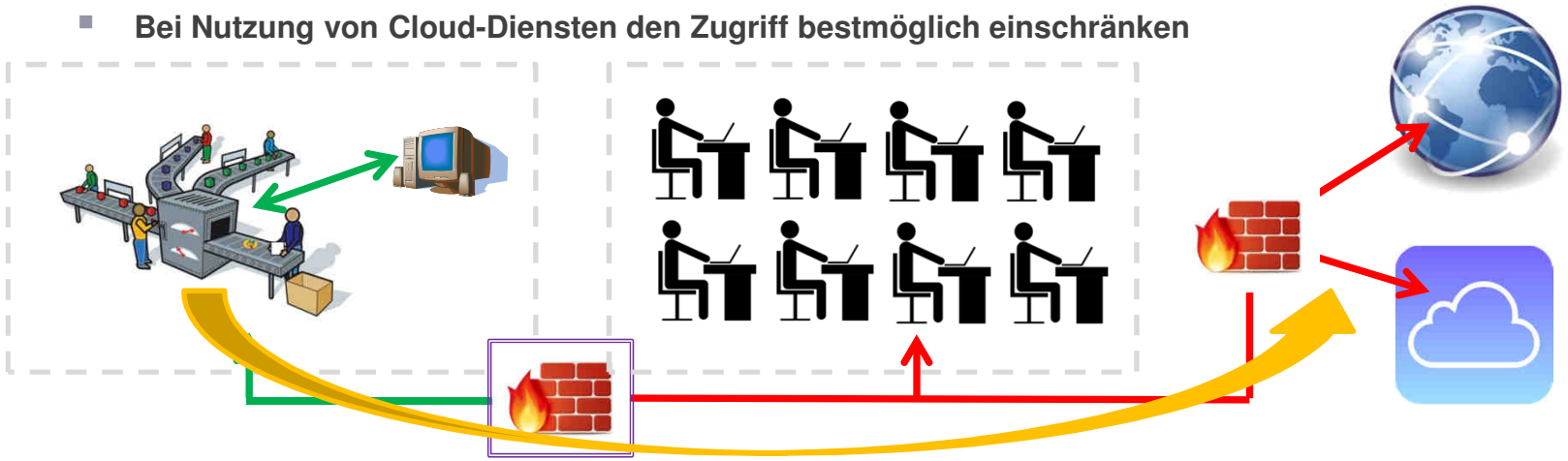
Schutz für Produktionsanlagen

- Beschränken der Zugriffsmöglichkeiten aus dem Office-Bereich auf das nötige Minimum
  - Office-PC‘s mit Zugriff auf die Produktion besonders schützen (z.B. kein Internet oder Mail)
  - Nur Protokolle / Ports freigeben, die auch tatsächlich benötigt werden

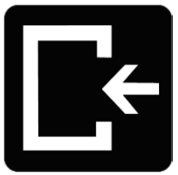


Schutz für Produktionsanlagen

- Zugriff aus der Produktion ins Internet oder zu Cloud-Diensten wenn möglich verhindern
  - Kein Internetzugang oder Mailverkehr auf PC‘s von Produktionsmaschinen
  - Bei Nutzung von Cloud-Diensten den Zugriff bestmöglich einschränken



Zugriffe von „außen“ - Fernwartung



- Komplexität der Anlagen steigt rasant
- Bei kleineren Unternehmen oder Außenstellen ist oft kein Fachpersonal zur Wartung / Diagnose vor Ort
- Die Verwendung von Fernwartungszugängen ist teilweise unumgänglich
  - Zur Fehlersuche durch den Hersteller oder zentrales Wartungspersonal
  - Zum Einbringen neuer Steuerungsprogramme
  - Zur Erweiterung von Funktionen

Fernwartung - Varianten

- Fernwartungs-Funktionen werden oft vom Anlagenhersteller ab Werk eingebaut
  - Telefon- oder ISDN Modems (sind in Neuanlagen kaum mehr zu finden)
  - Phone-Home Router
  - GSM-Modems mit SIM-Karte
  - VPN-Server

Fernwartung – Telefon/ISDN

- Telefon- oder ISDN Modems
  - Umgehen die vorhandenen IT-Sicherheitseinrichtungen
  - Sind zusätzliches Einfallstor für Bedrohungen von außen
  - Angriffe können sich auf des restliche Netzwerk unkontrolliert und unbemerkt ausbreiten

Fernwartung – Phone-Home Router

- Phone-Home Router
  - Nutzen einen ausgehende Internetverbindung um eine eingehende Verbindung aufzubauen
  - Umgehen ebenfalls die vorhandenen IT-Sicherheitseinrichtungen
  - Zugriffe sind für den Anlagenbetreiber kaum kontrollierbar
  - Als Gateway wird ein externer Dienstleister genutzt – wird dieser kompromittiert, stehen möglicherweise alle von ihm gehostete Verbindungen offen
  - Einzige Kontrollmöglichkeit besteht durch elektrisches Abschalten des Routers

Fernwartung – GSM-Modem/Router

- GSM-Modems/Router mit SIM-Karte
  - Funktionsweise und Risiken sind ähnlich wie beim Phone-Home Router
  - Die Geräte benötigen weder eine Anschlussleitung noch eine sichtbare Antenne
  - Das Vorhandensein eines solchen Geräts bleibt ggf. für den Anlagenbetreiber unbemerkt

Fernwartung – VPN-Server

- VPN-Server
  - Ist wahrscheinlich bereits in der IT-Umgebung vorhanden (z.B. für Teleworking …)
  - Die Kontrolle über Zugriffe liegt beim Anlagenbetreiber
  - Keine unkontrollierten oder unangekündigten Zugriffe von außen möglich
  - Zugänge sind einfach einzuschränken und zu deaktivieren
  - Protokollierung der Zugriffe ist möglich

Fernwartung - Tipps

- Tipps
  - Bereits vor Anschaffung einer Anlage mit dem Hersteller Fernwartungsregeln vereinbaren
  - Wenn technisch möglich, den Einsatz von Phone-Home Routern und GSM-Modems untersagen
  - Bei Inbetriebnahme einer neuen Anlage das Vorhandensein solcher Geräte prüfen (lassen)
  - VPN-Zugänge als bevorzugten Fernwartungsweg nutzen
  - Nicht benötigte Zugänge sperren und nur bei Notwendigkeit öffnen

IOT – das Internet der Dinge - privat

- Im Home/Privatbereich sind unzählige Anbieter und Dienste verfügbar
  - Überwachungskameras
  - Heizungssteuerungen
  - Türschlösser
- Zugriff und Bedienbarkeit vom Smartphone aus
- Nutzen einen Cloud-Server um den Zugriff zu ermöglichen
- Die Geräte selbst agieren wie Phone-Home Router

IOT – das Internet der Dinge - kommerziell

- Zunehmend sind IOT-Devices auch im kommerziellen und industriellen Umfeld zu finden
  - Sensoren und Messgeräte (z.B. Energiezähler, GPS-Tracker, Temperaturfühler ….)
  - Bis hin zu kompletten Einheiten zur Betriebsdatenerfassung
- Nutzen die Phone-Home Strategie und einen Cloudserver des jeweiligen Anbieters
- Abfrage der gespeicherten Daten meist über eine Webseite des Anbieters
- Anbieter stellen oft aufwändige Analysetools zur Verfügung

Sicherheit in der Cloud

- Kritische Fragen vor dem Einsatz von Cloud-Lösungen
  - Welche Daten liefere ich durch die Nutzung von Diensten oder IOT-Geräten in die Cloud
  - Sind diese Daten sensibel oder unternehmenskritisch ?
  - Lassen sich durch diese Daten Rückschlüsse auf das Unternehmen schließen ?
  - Sind personenbezogene Daten enthalten und unterliegen sie damit dem Datenschutz ?
  - Was bedeutet ein temporärer Ausfall oder die Einstellung des Dienstes für das Unternehmen ?

Sicherheit in der Cloud

- **Voraus gedacht …**
  - **Wie sicher sind die eigenen Daten eigentlich in der Cloud ?**
  - **Wo auf der Welt werden meine Daten gespeichert und wie kann ich das sicherstellen ?**
  - **Welche regionalen Datenschutzgesetzte liegen zugrunde und werden diese auch geachtet ?**
  - **Ist die (möglicherweise geforderte) eigene Aufbewahrungspflicht für Daten sichergestellt ?**
  - **Was passiert mit meinen IOT-Geräten, wenn es den Anbieter nicht mehr gibt ?**
  - **Bleiben die Rechte an den Daten im eigenen Unternehmen ?**

Die richtige Cloud ?

- Der richtige Cloud-Anbieter sollte / muß
  - kein unbekannter Player und am Markt etabliert sein
  - seine Dienste keinesfalls kostenlos anbieten
  - nach Möglichkeit seinen Sitz und seine Datencenter nachweislich in der Region haben
  - den Datenschutz nach lokalen Gesetzen einhalten
  - unbedingt die Möglichkeit bieten, alle Daten Maschinenlesbar zum Download bereitzustellen
  - Bei Vertragsende ein unwiderrufliches Löschen der Daten garantieren

Aus der Kriminalitäts-Statistik 2016

Quelle: http://www.bmi.gv.at/cms/BK/publikationen/krim_statistik/2016/Web_Sicherheit_2016.pdf

Danke für Ihre Aufmerksamkeit

Graf Markus

Quelle aller Logos und Piktogramme: Office Cliparts