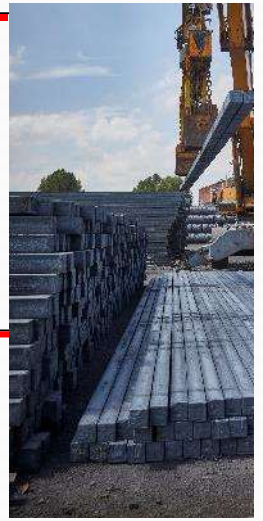
IT-Sicherheit
- ein Erfahrungsbericht -

Das Produktionsgelände der BSW

Vom Schrott zum Stahl



… zu Betonstahl und Walzdraht

Stahlwerk

Knüppel / Knüppelplatz

Stabstahlwalzwerk

51% Heißeinsatz (Ø 800°C)

60% vom Lager

Stoßofen 1 (Erdgas)

(1)

(3)

(4)

Betonstahl (10-40 mm)

444.000 t p/a

(1) Vorstraße
(2) Zwischenstraße
(3) Fertigblöcke
(4) Kühlstrecke

Drahtwalzwerk

89% Heißeinsatz (Ø 800°C)

20% vom Lager

Stoßofen 2 (Erdgas)

(1)

(2)

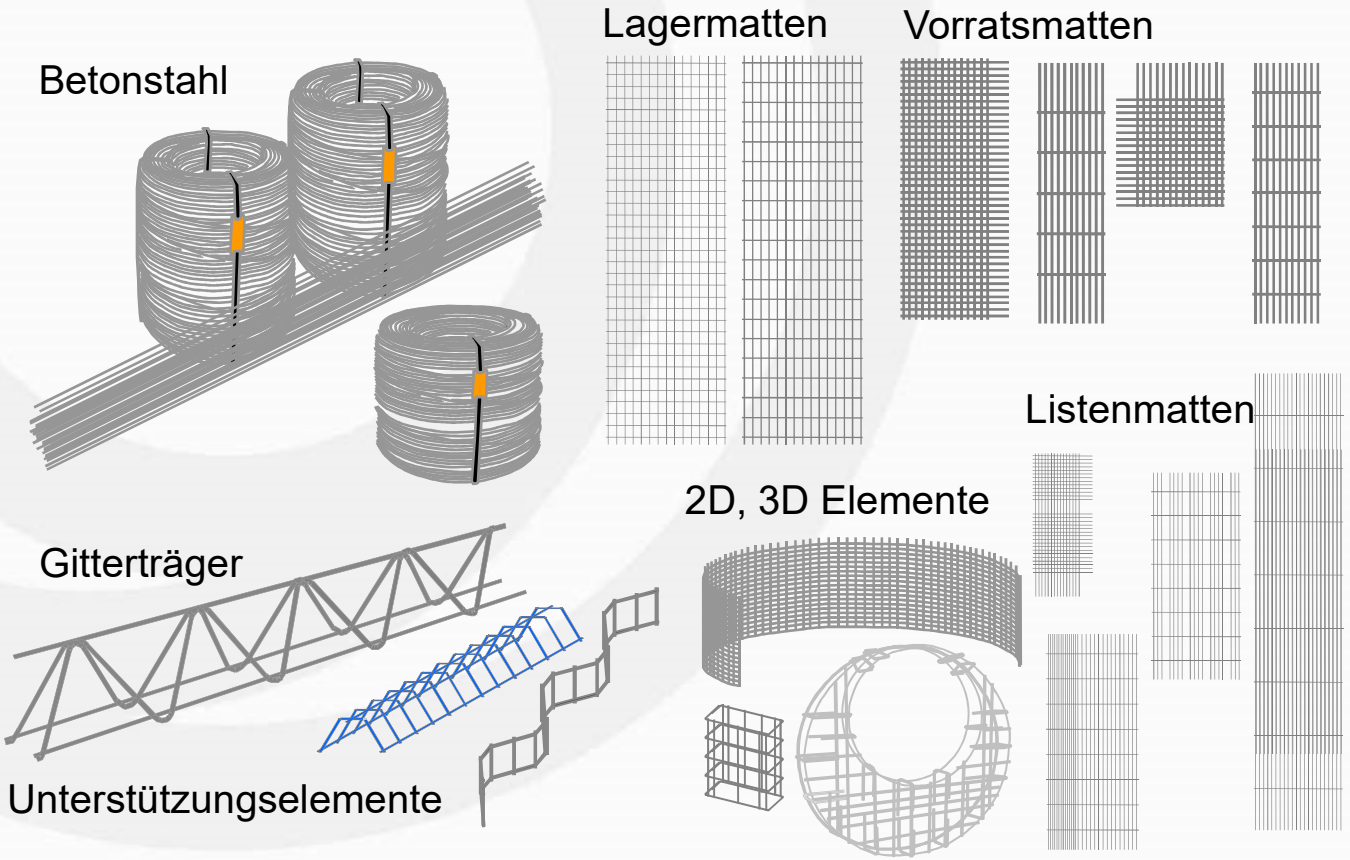
(3)

(4)

Walzdraht (5,5-20 mm)

1.174.000 t p/a

Wir sind der führende Lieferant für Bewehrungsprodukte in Deutschland



Produktions- und Absatzstandorte

ERFOLGSFAKTOR
LOGISTIK- UND VERTRIEBSKONZEPT

- Stahlproduktion
- Weiterverarbeitung
- Vertrieb

IT-Sicherheitsvorfall 20. April 2023

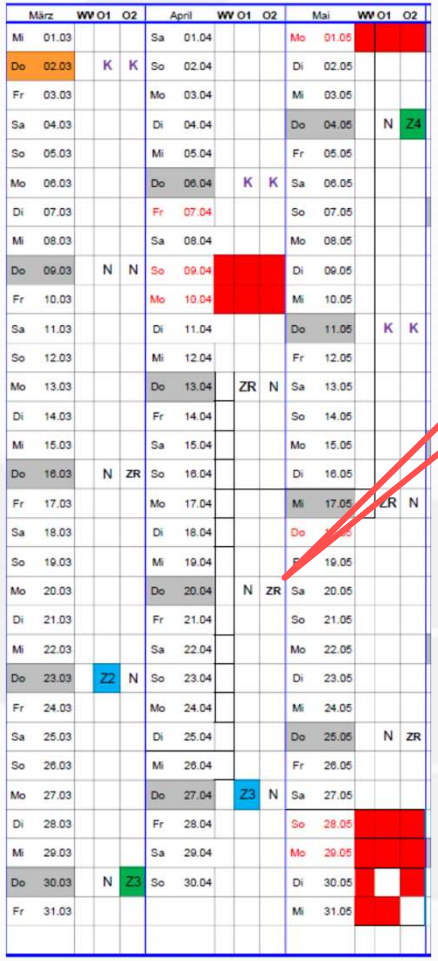
20. April 2023

- Gegen 04:00 Uhr EDV-Störung an Waage-Rechner
- => IT-Dienstbereitschaft verständigt
  => von zu Hause aufgeschaltet
  => sofort ins Werk gekommen.
- Gegen 06:30 Uhr: Mitarbeiter IT laufen durchs Werk und ziehen Netzwerkkabel aus Rechnern, Druckern, …
- MEF INO **Monat: 04.2023** **Produktionsübersicht V 438** Erstelldatum: 27.06.2023 07:00:04 Seite 1 von 1

	Walzwerk 1							Walzwerk 2									Stahlwerk							
Tag	Plan	Ist	kum Abw	Ø	TO/ HZ	TO/ BZ	Heiß %	Plan	Ist	kum Abw	Ø	TO/ HZ	TO/ BZ	kmh %			Plan	Ist	kum Abw	Anz Chrg	EO1	EO2	Gute Erz %	Tap /Tap
DI.18	1.885	1.901	-68	25,8	101	82	51	4.680	4.971	2.469	7,5	235	207	22	35	44	8.035	7.958	4.023	74	4.005	3.953	88,5	38,64
MI.19	1.980	1.896	-152	27,9	122	87	68	4.680	4.586	2.376	7,5	221	191	52	31	17	8.035	8.361	4.349	76	4.191	4.170	90,8	37,87
DO.20	1.600							2.880									3.850							
FR.21	1.700							3.960									8.035	642	-6.894	6	642	0	90,4	43,39
SA.22	2.040							4.500									8.035							
SO.23	2.040							5.170									8.035							
MO.24	2.040							4.700									7.735	3.514	-27.185	32	3.514	0	90,1	38,15
DI.25	1.700							5.640									8.035	4.144	-31.076	38	3.944	200	90,0	39,29
MI.26	2.040							4.700	1.210	-27.965	11,0			0	0	0	6.529	3.639	-33.966	34	988	2.651	88,7	40,40
DO.27	2.040							3.760	2.220	-29.505	11,0	186	156	0	0	0	3.850	4.540	-33.276	42	2.075	2.465	87,8	40,41
FR.28	1.200	2.937	******	19,1	202	148	0	4.510	4.165	-29.850	8,8	174	174	0	0	0	8.035	7.987	-33.324	73	3.970	4.017	89,1	39,00
SA.29	1.800	1.820	******	16,0	103	76	0	5.640	3.992	-31.498	8,5	166	166	0	0	0	8.035	8.090	-33.269	74	3.952	4.138	89,4	39,31
SO.30	1.725	1.858	******	16,0	112	81	0	5.405	3.698	-33.205	8,5	154	154	0	0	0	7.701	7.561	-33.408	69	3.851	3.710	90,4	38,39

Jahresplanung BSW: SW - WW - Donnerstags-Stillstandsplanung für 2023

= Beginn Walzkampagne
= Betriebsversammlung geplant
K = kurzer Stillstand zur Reinigung
= Produktionsstillstand gem. Schichtplan
Z = Zustellung O1
Z = Zustellung O2
= geplanter Produktionsstillstand
ZR = Zwischenreparatur
N = Normaler Stillstand
= Sommerstillstand



März	WW	O1	O2	April	WW	O1	O2	Mai	WW	O1	O2
Mi 01.03				Sa 01.04				Mo 01.05			
Do 02.03		K	K	So 02.04				Di 02.05			
Fr 03.03				Mo 03.04				Mi 03.05			
Sa 04.03				Di 04.04				Do 04.05		N	Z4
So 05.03				Mi 05.04				Fr 05.05			
Mo 06.03				Do 06.04		K	K	Sa 06.05			
Di 07.03				Fr 07.04				So 07.05			
Mi 08.03				Sa 08.04				Mo 08.05			
Do 09.03		N	N	So 09.04				Di 09.05			
Fr 10.03				Mo 10.04				Mi 10.05			
Sa 11.03				Di 11.04				Do 11.05		K	K
So 12.03				Mi 12.04				Fr 12.05			
Mo 13.03				Do 13.04		ZR	N	Sa 13.05			
Di 14.03				Fr 14.04				So 14.05			
Mi 15.03				Sa 15.04				Mo 15.05			
Do 16.03		N	ZR	So 16.04				Di 16.05			
Fr 17.03				Mo 17.04				Mi 17.05		ZR	N
Sa 18.03				Di 18.04				Do [illegible]			
So 19.03				Mi 19.04				Fr 19.05			
Mo 20.03				Do 20.04		N	ZR	Sa 20.05			
Di 21.03				Fr 21.04				So 21.05			
Mi 22.03				Sa 22.04				Mo 22.05			
Do 23.03		Z2	N	So 23.04				Di 23.05			
Fr 24.03				Mo 24.04				Mi 24.05			
Sa 25.03				Di 25.04				Do 25.05		N	ZR
So 26.03				Mi 26.04				Fr 26.05			
Mo 27.03				Do 27.04		Z3	N	Sa 27.05			
Di 28.03				Fr 28.04				So 28.05			
Mi 29.03				Sa 29.04				Mo 29.05			
Do 30.03		N	Z3	So 30.04				Di 30.05			
Fr 31.03								Mi 31.05			

Mi	19.04		
Do	20.04	N	ZR
Fr	21.04		

- Öfen schalten gegen 03:30 und 03:50 Uhr ab
- Stranggußanlagen gegen 05:15 Uhr ausgelaufen (ohne Visu)
- Walzwerke kontrolliert runtergefahren,
  aber teilweise „Blindflug“ (Bildschirme schwarz)
- Drahtwerke lauffähig
  (Maschinen „Netzwerk-unabhängig“),
  aber Stillstand wegen fehlender Daten:
  Bestand, Einkauf, Vertrieb, Produktionsplanung, …

20. April 2023

Kehl, 20. April 2023

Badische Stahlwerke von unautorisiertem Netzwerk-Zugriff betroffen

Sehr geehrte Damen und Herren,
liebe Kundinnen und Kunden,
liebe Geschäftspartner,

die Badische Stahlwerke GmbH untersucht aktuell mit hoher Priorität einen unautorisierten Zugriff auf das IT-Netzwerk der Unternehmensgruppe. Der Zugriff wurde am 20.04.2023 identifiziert, woraufhin wir unverzüglich relevante Systeme isoliert und kontrolliert abgeschaltet haben.

Gemeinsam mit externen Experten haben wir eine umfassende Überprüfung unserer Systeme gestartet, die aktuell noch andauert. Durch den Zugriff und die Abschaltung der Systeme sind wir temporär per E-Mail und Festnetz-Telefon nicht erreichbar.

Davon sind folgende Unternehmen der Gruppe betroffen:
Badische Stahlwerke GmbH, BSW Anlagenbau und Ausbildung GmbH,
BSW Anlagentechnik GmbH, Badische Stahl-Engineering GmbH,
BSW Stahl-Nebenprodukte GmbH, BCT Technology AG, BCT Technology GmbH
sowie alle Drahtverarbeitungsbetriebe.

Wie es zu dem Vorfall kommen konnte, ist noch unklar. Die Sicherheitsstandards unserer IT-Systeme sind sehr hoch und die Sicherheit Ihrer Daten hat für uns oberste Priorität. Wir haben alle zuständigen Behörden über den Vorfall informiert und arbeiten bei der Aufklärung des Vorfalls eng mit diesen zusammen.

Die Analysen dauern noch an und wir versichern, dass wir alle Anstrengungen unternehmen, um den Vorfall umfassend und schnell aufzuklären. Sobald uns weitere relevante Erkenntnisse vorliegen, werden wir hierzu umgehend informieren.

Wir danken Ihnen für Ihr Verständnis in dieser Situation!

Mit freundlichen Grüßen
Ihre Badische Stahlwerke GmbH

Florian Glück Markus Menges Andreas Volkert

Hackerangriff auf Badische Stahlwerke in Kehl

Betroffene Systeme vorübergehend abgeschaltet

Kehl (ts/ys/ba). Auf das Netzwerk der Badische Stahlwerke GmbH in Kehl hat es am Donnerstag einen Hackerangriff gegeben. Das bestätigte die Polizei in Offenburg. Das Unternehmen selbst weist auf seiner Homepage auf den „unautorisierten Zugriff" hin.

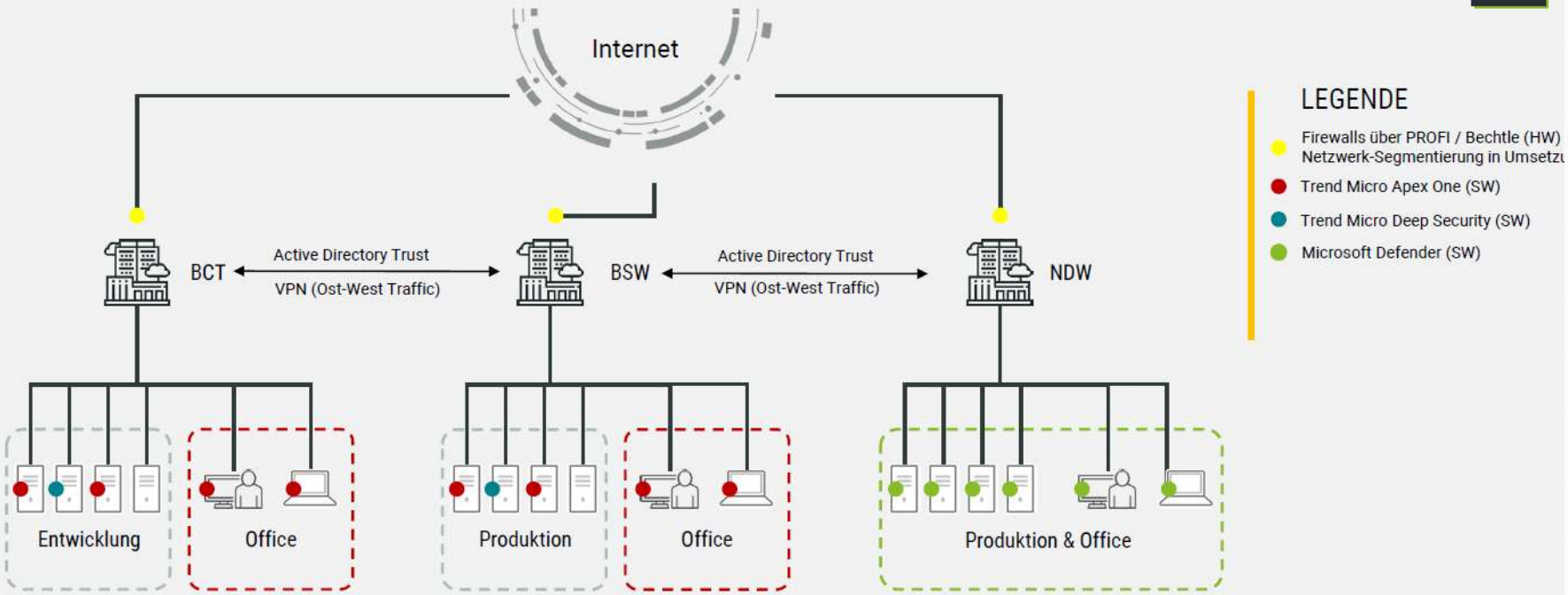
Nicht erreichbar

Demnach wurden die betroffenen Systeme abgeschaltet, weshalb Mitarbeiter vorübergehend per E-Mail und Festnetz-Telefon nicht erreichbar seien. „Wir arbeiten derzeit mit Hochdruck daran, den Vorfall umfassend und schnell aufzuklären", heißt es. Wir haben das Unternehmen für eine Stellungnahme angefragt.

Hacker hatten es am Donnerstag auf die Badischen Stahlwerke Kehl abgesehen.
Symbolfoto: K.-J. Hildenbrand/dpa

Die Ermittlungen in diesem Fall sind laut Polizei angelaufen. Nähere Informationen gibt es noch nicht. Rund 850 Menschen sind in Kehl bei den Badischen Stahlwerken beschäftigt.

SITUATION BEI INFIZIERUNG



⇒ Ursache: Phishing Mail in einem der Drahtwerke

⇒ Ziel: Zerstörung und Umsatz
=> „Ticket“ hinterlegt mit Aufforderung zu Kontakt
=> Recherche im Darknet: - kein Datenabfluß,
- keine offene Erpressung

- Kommunikation sicher stellen:
  => Telefone nicht in Funktion (VoIP)
  => E-Mail über MS-Outlook außer Funktion
  => Berichtswesen außer Funktion:
  - Prozessdaten
  - Schichtberichte
  - Arbeitsschutz-Reporting
- MS-Teams auf Mobiltelefonen einrichten
- Mobiltelefone als Hotspots einrichten
  (IT stellt Verträge auf unbegrenztes Datenvolumen ein)
  => E-Mail-Adressen über gmx generieren
  => Namenscodex festlegen, z.B. *BSW_AS@gmx.de*
- Funkgeräte und Faxgeräte zur Prozessdaten-Weitergabe verteilen
- Notfallmanagement sicherstellen
- Alte Hardcopies gebrauchsfähig machen (TippEx) und als Kopiervorlage verteilen
  => Reporting handschriftlich

- Krisenstab täglich 16:00 Uhr
  => Information Führungskräfte via Teams
- Forensik starten: Seit wann infiziert?
  => Rücksicherung von Daten ab wann möglich?
- Notfallkonzept Versand: Täglich visuelle Bestandsaufnahme
- Personal: Zeiterfassung speichert, Zeitkonten nutzen

Status IT-Infrastruktur:

- Linux- (Produktions-) Systeme und Insel-Windows-Systeme nicht befallen
- Windows-Rechner in 3 Stufen:
  1. Im Netz integrierte und zum Zeitpunkt des Angriffs eingeschaltete Rechner verschlüsselt
  2. Virenscanner detektiert bis zu 7 Viren
     => nicht benutzbar
  3. Rechner offensichtlich nicht befallen

24./25. April 2023

Produktion läuft wieder teilweise

Hackerangriff belastet Badische Stahlwerke

Kehl (all). Nach einem Hackerangriff am vergangenen Donnerstag läuft der Betrieb in den Badischen Stahlwerken in Kehl (BSW) nach wie vor nur eingeschränkt. Das hat eine Unternehmenssprecherin am Montag auf Anfrage der MITTELBADISCHEN PRESSE erklärt. Durch die Abschaltung und Überprüfung der Systeme seien die Badischen Stahlwerke vorübergehend per E-Mail und Festnetz-Telefon nicht erreichbar. Die Produktion sei bereits am Freitag teilweise wieder aufgenommen worden.

Bereits am Freitag hatte die Polizei den Angriff auf die IT-Infrastruktur des 850 Mitarbeiter zählenden Unternehmens auf Nachfrage bestätigt, die BSW selbst hielten sich zu dem Zeitpunkt noch bedeckt. „Die Ermittlungen in Zusammenarbeit mit Behörden und Security-Experten sind noch in einem sehr frühen Stadium, weshalb keine Details kommuniziert werden dürfen", begründet die Sprecherin die Zurückhaltung.

Angriffe auf Computersysteme mit Verschlüsselungstrojanern (Ransomware) gelten seit Jahren als die gravierendste Bedrohung der Cybersicherheit. Dabei blockiert eingeschleuste Schadsoftware die Unternehmen oder legt ihre Infrastruktur lahm. Geschädigte können so nicht mehr auf ihre Daten zugreifen. Die Täter verlangen Lösegeld (englisch „ransom") für die Entschlüsselung. Abgerechnet wird oft in der Digitalwährung Bitcoin.

Systeme abgeschaltet

Laut der BSW-Sprecherin gibt es derzeit keine Erkenntnisse darüber, ob bei dem Hackerangriff Daten abgeflossen sind. Das Unternehmen habe unverzüglich reagiert und alle relevanten Systeme isoliert und kontrolliert abgeschaltet. „Die Sicherheitsstandards unserer IT-Systeme sind sehr hoch, und die Sicherheit von Daten hat für uns oberste Priorität. Wir setzen jetzt alles daran, den Vorfall aufzuklären und unsere volle Betriebsfähigkeit so schnell wie möglich wieder herzustellen", betont BSW-Geschäftsführer Markus Menges in einer Stellungnahme des Unternehmens.

IT-Infrastruktur:

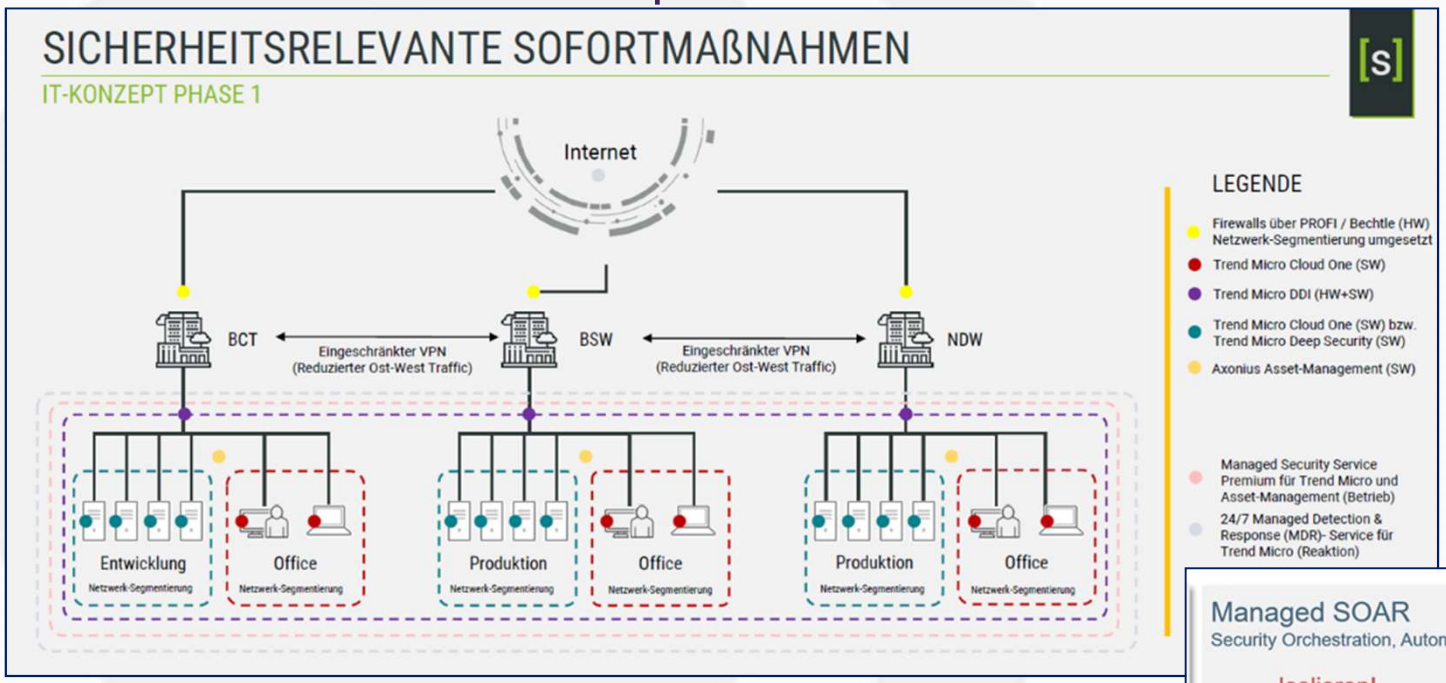
Teilung Netzwerk in rote/gelbe/grüne Zone:

- Rote Zone:
  Systeme, die nach dem 31.01.23 eingeschaltet waren („Inkubationszeit").
  Am 20.04. nicht eingeschaltete Rechner überprüft und in roter Zone weiter betrieben
- Gelb:
  Quarantäne nach Wiederherstellung aus Backup zum Testen/Scannen
- Grün = produktiv:
  neu installierte bzw. wiedergestellte, komplett getestete Systeme

Ab Mai 2023

- Kauf von 150 neuen Rechnern (Laptops)
  => neu aufsetzen,
  => Ausgabe gemäß Prioritätenliste
- Einsammeln der getauschten Rechner, Neuinstallation (Aussondern aller nicht Windows 11 fähigen Rechner), ca. 1000 Systeme rollierend getauscht
- „Alltags-Probleme“ lösen:
  - WLAN wieder herstellen
  - Drucker-Zugriff
  - Easy-Key Fahrzeug System
  - Fahrzeug-Waage
  - Besucherverwaltung / Fremdfirmenmgt.
  - QS-Produktzertifikate sicher stellen
- Neues IT-Sicherheitskonzept aufbauen

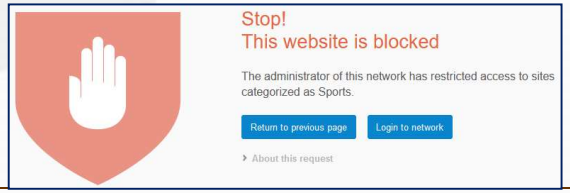
- Neues IT-Sicherheitskonzept

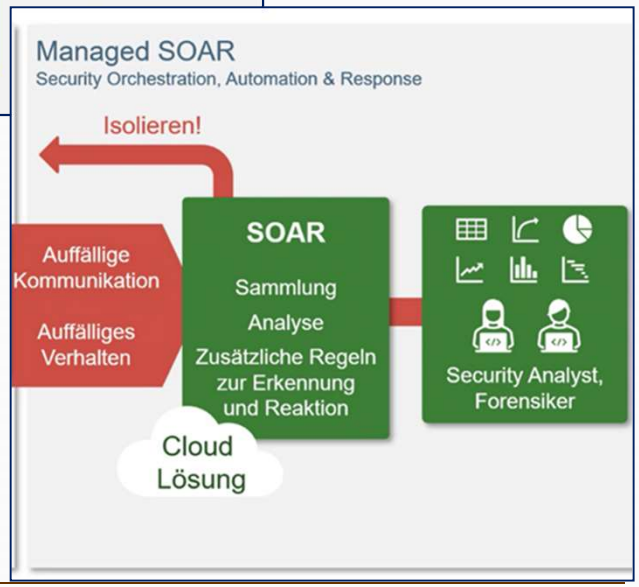


⇒ Segmentierung der Netzwerke nach Abteilung / Räumlichkeit

⇒ KI-basierte Nutzer-Verhalten Analyse

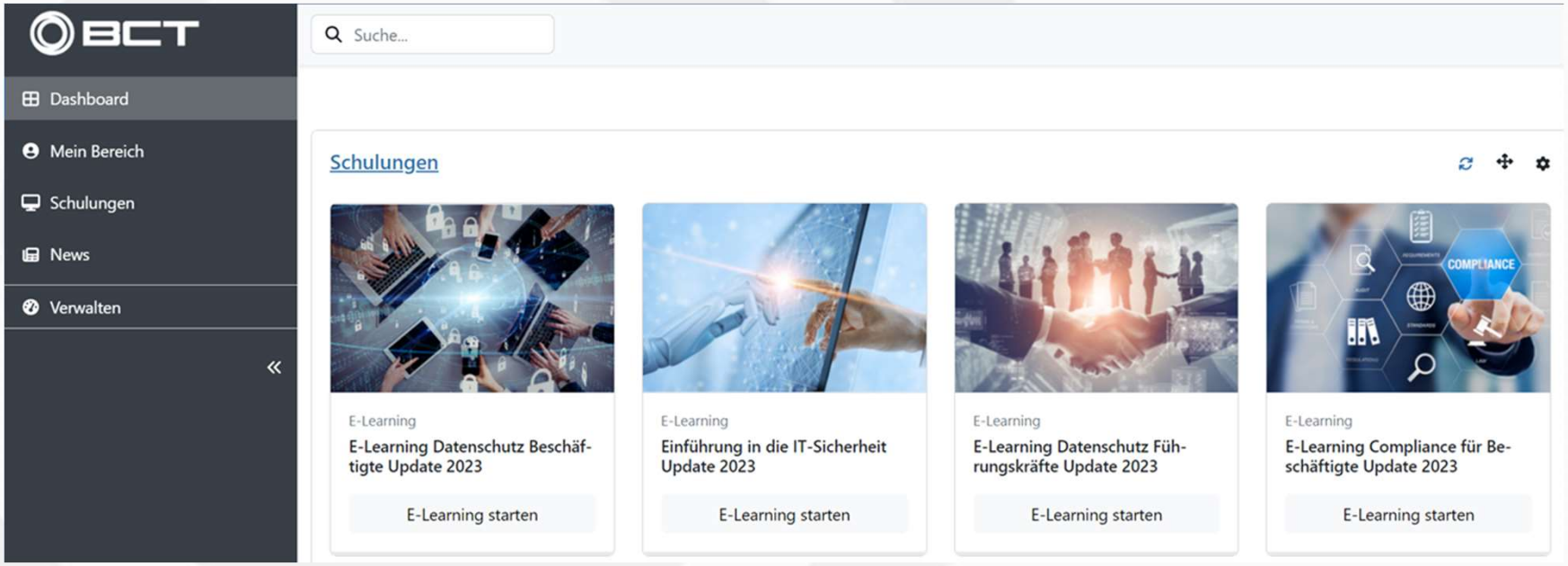
⇒ Internet-Einschränkung





- Mitarbeiter-Training und –Sensibilisierung

  ⇒ E-Learning Module



  ⇒ Real-Tests mit eigenen Phishing-Mails

Zusammenfassung

- IT kostet Geld!
- IT wird als strategisches Unternehmensziel etabliert
  => Schaffung Position „CIO“
  => IT-Sicherheitsfachkraft
  => IT-Ausbilder
- Das schwächste Glied ist immer noch „der User“
- Nur noch namentliche Accounts
- Arbeitsschutz ist in zweierlei Hinsicht bei der IT-Sicherheit zu bedenken:
  - Unbefugte Steuerung von Anlagen;
  - Gefährdung durch Ausfall von Sicherheitssystemen

baustahlgewebe | BSW Badische Stahlwerke GmbH | SWB Dienstleistungsgesellschaft mbH

MITARBEITERINFORMATION

Aushang **bis 29.02.2024**

Mit „bewehrter“ IT in die Zukunft

Sehr geehrte Beschäftige,

wie Sie alle noch in Erinnerung haben, wurde die gesamte Unternehmensgruppe am 20.04.2023 Opfer einer Cyber-Attacke.

Dank dem enormen Engagement aller Beteiligten konnten wir recht schnell wieder produzieren. Auch wenn die Einschränkungen in der täglichen Routine mittlerweile gering sind, so beschäftigen uns die Nachwirkungen an allen Standorten weiterhin.

Durch diese Cyber-Attacke wurde deutlich aufgezeigt, dass IT und IT-Sicherheit ganzheitlich in der Unternehmensgruppe behandelt werden müssen. Ohne eine zukunftsfähige und widerstandsfähige IT ist unsere Wertschöpfung nicht gesichert möglich.
Deshalb haben wir in den letzten Wochen einen IT-Strategie-Prozess mit Teilnehmern aus Eberbach & Kehl durchgeführt.
Dabei wurden einige Themen identifiziert, an denen wir in den nächsten Monaten intensiv arbeiten werden, wie zum Beispiel:
IT-Sicherheit inkl. der Produktionsanlagen, **MES** (Produktionsleitsystem), Standardisierung in den **ERP-Systemen**, IT-Unterstützung technischer Prozesse (z.B. Instandhaltung, technische Dokumentation), **Microsoft 365** (Cloud) aber auch an der Sicherstellung ausreichender **IT-Ressourcen**.

Details hierzu werden wir turnusgemäß in den bestehenden Besprechungsformaten berichten.

Kehl/Rhein, 30. Januar 2024

Kai Weber Florian Glück Andreas Volkert Klaus Erdrich

Fragen & Anmerkungen