atp magazin

SONDERDRUCK

Transforming Automation
Ausgabe 1-2/2023

OT-Security: Was tun bei Cyberangriffen auf die OT?

Walter Speth, Erwin Kruschitz

Die Antwort auf die Frage in der Überschrift ist denkbar einfach: Dem Notfallhandbuch folgen. Das muss natürlich ausgearbeitet sein und im Folgenden soll es um den Teil gehen, der Auskunft darüber gibt, ob die Verbindung der OT zur IT zu trennen ist und welche Kriterien Anlass dazu geben, dies zu tun. Immerhin steht zu befürchten, dass mit der Trennung mehr Schaden als Schutz entsteht.

Formulieren wir die Frage also um: Wann ist eine Trennung der Kommunikation an der Schnittstelle der OT zur IT zu verantworten? Auch das ist natürlich im Vorfeld überlegt worden, nachdem die Risikoanalyse angestrengt wurde und auch über Systeme der Angriffserkennung entschieden wurde, die als Teil der Maßnahmen implementiert wurden. Jedoch würde keinem solchen Erkennungssystem erlaubt werden, eine Trennung der Kommunikation zwischen IT und OT vorzunehmen. Sie liefern Hinweise auf „Anomalien“ – also mutmaßliche Angriffe, die von verantwortlichen Mitarbeitenden in der Produktion wahrgenommen (oder „observiert“) werden wie all die anderen irregulären Ereignisse auch, die sich oft der automatischen Erkennung entziehen.

Auswirkungen eines Cybernotfalls gering halten, aber wie?

Im Folgenden wird ein Ansatz vorgestellt, wie solche Beobachtungen unter Einbeziehung des Notfallhandbuchs in (manuelle) Aktionen münden können. In diesem Beispiel fokussieren sich die Aktionen auf die IT-OT-Kommunikation, welche in einer Form beeinflusst wird, die die Auswirkung eines Cybernotfalls gering und die Steuerungswirkung des Notfallteams hoch halten soll.

Nehmen wir beispielhaft an, die Kommunikationsverbindungen zwischen IT-Systemen und OT-Systemen stellten sich wie in Tabelle 1 aufgeführt dar.

Die Zahlen entsprechen verschiedenen Situationen, die sich als Folge eines Ereignisses z. B. eines Cyber-Angriffs einstellen können. Wir wollen Sie als „Alarmstufen“ bezeichnen und geben der kritischsten Situation die kleinste Zahl (1). Damit wird bei einer Eskalation schnell klar, wie nahe man am Cyber-GAU ist, während bei aufsteigender Zählung wie etwa der Richterskala für Erdbebenstärken, leicht Unsicherheit bestehen würde, wie hoch gezählt werden könne und damit, wie schlimm es denn bereits sei.

Betrachten wir die Schwere der Situation differenziert, wäre auch eine Trennung differenziert durchzuführen. Ausgehend von OT versus IT, also zwei Netzwerksegmenten an einer Firewall, lassen sich die folgenden Überlegungen auf mehrere Netzwerksegmente erweitern. Gleich bleibt, dass Systeme in einem Segment mit Systemen im anderen egment kommunizieren (dürfen), weil die

Tabelle 1: Die Verbindungen zwischen OT- und IT-Systemen.

Die Kommunikationsverbindungen sind unterbunden, wenn die Alarmstufe gleich oder kleiner als die angegebene Zahl ist.		IT-Systeme					
		ERP-Produktionsplanung	Remote Access	Patch Management	Backup	ERP-Materialwirtschaft	Data Historian/BDIS
OT-Systeme	Bedien-Beobachtung		3	5	5	2	3
	PLS-Engineering		6	5	4		
	PLS-Steuerungsebene		5			2	5
	SIS-Steuerungsebene					2	
	Rezeptsteuerung	3	4	5	4	2	3
	Rezeptur-Erstellung		6	5	5		

Tabelle 2: Eine Übersicht über mögliche Cybernotfall-Situationen.

Alarmstufe	Lage-Bezeichnung	Auswirkungen
1	Extremer Störfall	Tote und Verletzte in der Umgebung als Folge einer offensichtlichen Cyber-Attacke.
2	Störfall	Tote und Verletzte in der Anlage bzw. am Standort als Folge einer offensichtlichen Cyber-Attacke.
3	Hohe Gefahrenlage	Produktionsausfall oder Ausfall der funktionalen Sicherheit oder behördlich auferlegter Produktionsstopp.
4	Gefahrenlage	Produktion läuft, logistische Ausfälle bei Erzeugnissen oder Rohstoffen.
5	Eingeschränkter Regelbetrieb	Produktion läuft, keine Feststellung des Zustands der Anlage bzw. der Qualität des Produktes.
6	Verdacht auf Gefahrenlage	Produktion läuft, verstärktes Personal in der Anlage, auch externe bzw. Behördenvertreter:innen.
	Regelbetrieb	Produktion läuft oder Anlagenstillstand zwecks Wartung.

Tabelle 3: Gewichtung der Alarmstufen.

Alarmstufe	Gewicht	Anzeigen-Farbe
1	>1000	Violett, Funkelfeuer
2	800-1000	Blau, Blinklicht
3	600-800	Rot, auf-/Abschwellend
4	400-600	Orange, Dauerlicht
5	200-400	Gelb, Dauerlicht
6	100-200	Grün und Gelb im Wechsel
(Regelbetrieb)	<100	Grün, Dauerlicht

Firewall in ihrem Regelsatz den jeweiligen Datenfluss erlaubt. Wenn man nun die Gefahrenlage in Stufen einschätzt, würde man auch die einzelnen Kommunikationsverbindungen mit wachsender Stufe (also sinkender Zahl) aus dem Regelsatz entfernen und damit je Stufe zu einem angemessenen eigenen Regelsatz finden. Schlussendlich braucht es eine Firewall, die mehrere Regesätze und eine Umschaltung zwischen diesen auch ermöglicht.

Exemplarisch nutzen wir die Auflistung aus Tabelle 2. Dabei ist wichtig, dass nicht (mutmaßliche) Cyber-Situationen herangezogen werden, sondern Aspekte der Produktion, Lieferfähigkeit und Sicherheit für Personal, Bevölkerung und Umwelt einbezogen werden.

Den einzelnen Alarmstufen würden Punkte (Gewichte) zugeordnet (s. Tabelle 3), die – sollten sie von den Gewichten der Beobachtungen in Summe dann erreicht worden sein – zu der Einstufung (Alarmstufe) führen. Die Situation sollte in der Leitwarte allen sofort einsichtig sein, was eines gewissen Trainings (Notfallübung) und natürlich einer Darstellung bedarf, die akustisch oder optisch vorgenommen wird.

Bevor umgeschaltet wird, ist auch noch zu klären, wer die Umschaltung der Regelsätze in der Firewall durchführen darf. Wir gehen von einem technischen System aus, das Anwenderinnen und Anwender durch biometrische Überprüfung (hinterlegte Gesichtsbilder oder Fingerabdrücke) als berechtigt für die jeweilige Gefahrenlage authentifiziert, bevor es die per Eingabe gewünschte Umschaltung auf einen gewissen Regelsatz durchführt. Die Stärke der Authentifizierung kann mit der Alarmstufe wachsen und die Berechtigung kann von der Alarmstufe abhängig sein.

Was aber, wenn sich die befugte Person gar nicht in der Leitwarte aufhält, sondern sich etwa telefonisch meldet? Die technische Lösung sieht vor, dass dann von ihr ein Code übermittelt wird, der überprüft werden kann, ob sie zu der Alarmstufe berechtigt ist und es wird ein Code sein, der auf ein wechselndes Challenge der Lösung passt, also jedes Mal neu generiert wird.

Zunächst muss festgestellt werden, ob ein Angriff besteht und wie schwerwiegend er ist. Im Notfallhandbuch wäre eine Auflistung zu finden, die im Verdachtsfall abgeprüft würde, wie etwa Tabelle 4 zeigt. Dabei wird die „Beobachtung“ als *Indicator of Compromise* (IoC) bezeichnet.

Zu sehen ist, dass die Schwere der Beobachtung („Gewichtung“) auch je nach „Konfiguration“ des Anlagenzustands durchaus unterschiedlich beurteilt werden kann und soll. Wir haben als Konfigurationen den Regelbetrieb und den Wartungsbetrieb gewählt.

Wer darf einen Cybernotfall melden?

Wenden wir uns der Frage zu, wer denn eigentlich befugt und befähigt ist, einen IoC zu melden. Auch das gehört ins Notfallhandbuch und natürlich wird je nach Security-Kompetenz gewichtet, meist nach Rollen, in Einzelfällen auch nach Namen,

Tabelle 4: Mögliche Auflistung von Beobachtungen (*Indicators of Compromise*).

Regelbetrieb	Wartungsbetrieb	Indicator of Compromise
1000	500	Leitwarte fremdbesetzt
600	100	Integrität der sicherheitsgerichteten Steuerung nicht mehr gewährleistet
500	100	Unbekannte Anzeigen auf den Workstations
450	100	Hinweise auf eingeloggte fremde Benutzer
420	10	Unerklärlicher Ausfall/Stillstand von Systemen/Linien
200	10	Grenzwertüberschreitung von Prozessparametern
180	10	Häufige Abstürze von Server-Systemen
160	10	Hinweise vom Firewall-Monitoring
80	10	Malware auf vielen Systemen erkannt, Auswirkung schadhaft
60	10	SIEM-System löst Alarme aus
50	50	Riskante Schwachstellen an Produktionssystemen werden bei Angriffen auf vergleichbare Anlagen bereits ausgenutzt
40	10	Malware auf einigen wenigen OT-Systemen erkannt, Auswirkung unklar
30	30	Riskante Schwachstellen an Produktionssystemen erkannt, für die Exploits bekanntermaßen existieren
10	10	Verdacht auf Gefahrenlage durch Medienberichte, behördliche Information
0	0	Es bestehen keine Verdachtsmomente

etwa *Security Operations Center* (3), *Security Officer* (3), *Anlagenfahrer* (1), *Wartungsingenieur* (3), *IT* (2), *Firewall-Betreiber* (1), wobei die Zahlen in Klammern die Gewichtung bilden. Eine Änderung der Alarmstufe würde erst ausgerufen werden, wenn ein Quorum zustande käme, wobei je Rolle nur ein Votum gezählt würde, auch wenn es mehrere Personen gäbe, die die Rolle innehaben und sich äußern. Das für die auszurufende Alarmstufe erforderliche Quorum wäre im Notfallhandbuch nachzulesen.

Als *Observer* werden Personen angenommen, keine Systeme wie SIEM oder TI (*Threat Intelligence*), denn es geht um verantwortliche Entscheidungen und niemand könnte ein System zur Verantwortung ziehen. Wohl aber werden die Systeme unter den Beobachtern (Oberservern) aufgeführt und die Ausgaben solcher Systeme (Alarme) unter den Beobachtungen (IoC) genannt.

Wenn die hier aufgeführten Tabellen in der Notfallplanung gemäß der betrachteten Produktionsanlage aufgestellt sind, können Sie im Verdachtsfall anhand eines Vorgehens genutzt werden, das Abbildung 1 exemplarisch zeigt und die dann ebenfalls ins Notfallhandbuch gehört.

Validierung des Vorgehens

Anhand eines konstruierten Beispiels soll dieses Vorgehen verprobt werden. Im Regelbetrieb (also keine der Alarmstufen 1-6) bemerkt das Anlagenpersonal einen Dampfeintritt in den Reaktor, nachdem das Prozessleitsystem sie über eine Temperaturerhöhung informierte, die eine gesetzte Schwelle überschreitet. Offenbar ist das Dampfeintrittsventil geöffnet, das in diesem Produktionsschritt geschlossen sein sollte. Sie stellen das Dampfeintrittsventil unter Beobachtung, hegen aber keinen Verdacht auf eine Cyber-Sabotage als mögliche Ursache.

Die Situation wiederholt sich, aber das Ventil lässt sich über die Bedienstation nun nicht mehr schließen. Ebenso wenig wie das Ventil zur Reduzierung des Füllstands. Der Kontrollverlust führt zu einem ersten Anfangsverdacht. Die betrieblichen Ingenieur:innen werden informiert, um zu unterstützen. Das Notfallprotokoll wird herangezogen:

a. Ausgangssituation „Regelbetrieb“ wird festgestellt und notiert.

b. Als Beobachter wird die Rolle *Anlagenfahrer* mit Gewicht 1 festgestellt und notiert.

c. Die Beobachtung „Grenzwertüberschreitung“ (Gewicht 200 Punkte) führt nach der Gewichtung 1 zur Alarmstufe 6.

Jeder und damit eben auch das Anlagenpersonal sind berechtigt, die Alarmstufe 6 aufzurufen. Sie schalten die IT-OT-Verbindung um und verlieren die Möglichkeit der Unterstützung per Fernwartung für zwei IT-Systeme. Das Notfallhandbuch verlangt eine Überprüfung der Situation nach zwei Stunden. Die Hoffnung ist, dass die Ingenieur:innen mit Unterstützung durch den Hersteller des Prozessleitsystems bis dahin den Kontrollverlust beheben können und auf Regelbetrieb zurückgestellt wird. Die Annahme ist, dass ein Hacker über den Fernwartungszugang einbrechen und „herumspielen“ konnte.

Tatsächlich ist die Situation für die Beteiligten einigermaßen aufregend, es wird in den nächsten zwei Stunden viel

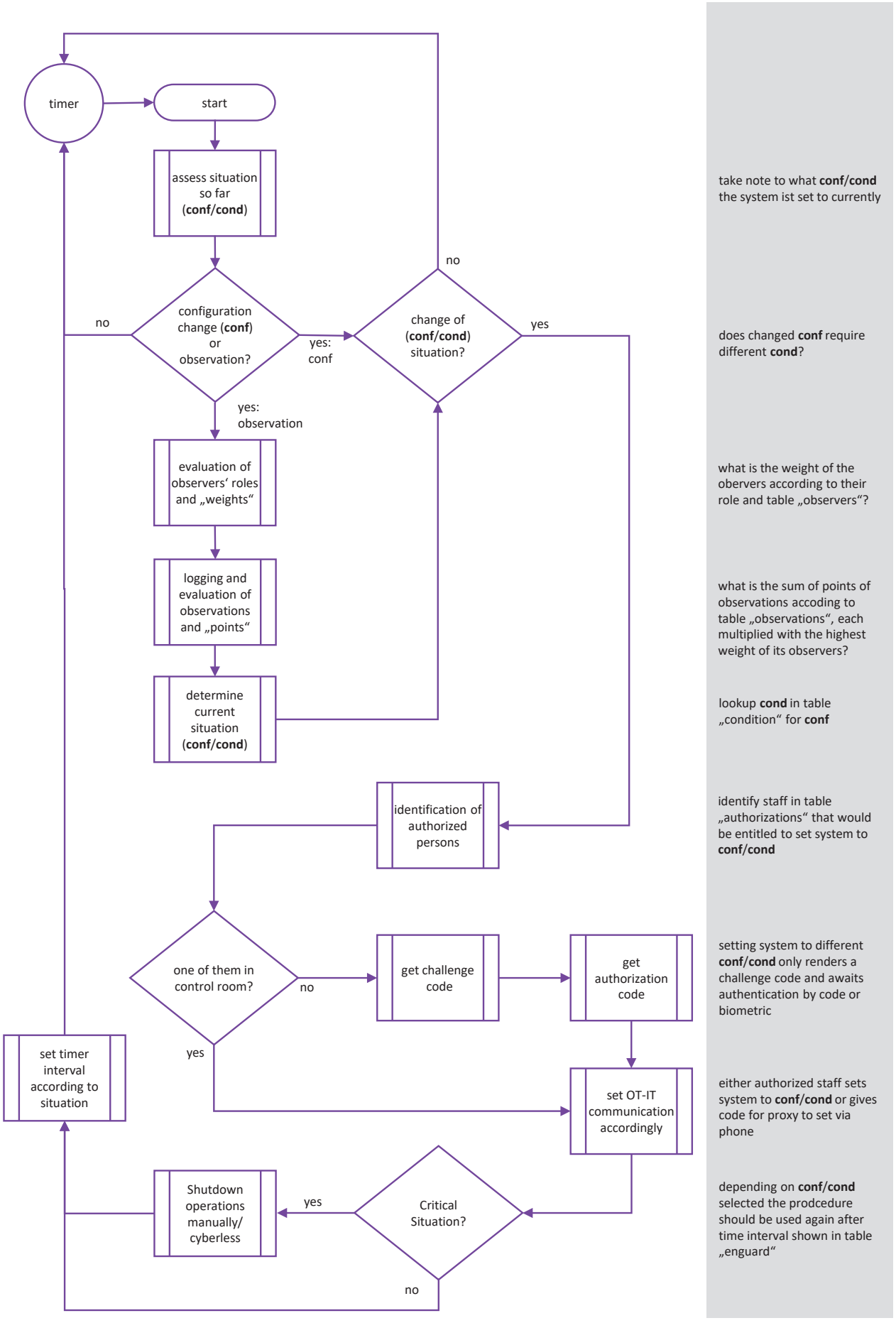

Abbildung 1: Flowchart für das Vorgehen während eines Cybernotfalls.

informiert und kommuniziert und es kommen Rückfragen von externen Service-Unternehmen (denen der Fernzugang nun nicht möglich ist) und dem Standort-Verantwortlichen. So erfährt man von weiteren Merkwürdigkeiten: Vom Lager erfährt man, dass die Rohstoff-Zulieferung schon den ganzen Tag stagniere, im Lager gebe es seit Stunden Probleme mit Barcode-Scannern, die so noch nie aufgetreten seien und offenbar helfe es auch nicht, die Barcodes händisch zu erfassen, denn die LKW-Waage berichte immer 0Kg, so dass eine Auslieferung nicht möglich sei. Das Flussdiagramm erneut durchlaufend, bekommt die Beobachtung ein Gewicht von 420 Punkten die anlagenfernen Beobachter aber nur ein Gewicht von 0.8 Punkten, was im Produkt zu Alarmstufe 5 führt. Der inzwischen anwesende Bereichsverantwortliche ist biometrisch mit Gesichtsbild registriert und die Erhöhung der Alarmstufe wird vom System anerkannt. Damit verlieren Patch-Management, Backup für Bedien-Beobachtungsstationen und Rezeptur-Erstellung die Kommunikationsmöglichkeit zur PLS-Steuerung wie auch der Data-Historian.

Das Anlagenpersonal und der Bereichsingenieur :innen nehmen nach einiger Zeit wahr, dass die gesamte Anlage anhält, weil die funktionale Sicherheit dies erzwingt. Eine schnelle Abfrage aller relevanten Sensor-Werte zeigt aber, dass es keinen technischen Grund dafür gibt. Die Beobachtung mit einem Gewicht von 600 Punkten und dem Bereichsverantwortlichen als Beobachter mit einem Gewicht von 1.2 ergibt mit 720 Punkten eine Alarmstufe 3. Dem muss die bisherige Wertung nicht hinzuaddiert werden, denn wie eine Rückfrage bei den anlagenfremden MItarbeitenden bestätigt, war eine ad-hoc-Änderung in der Infrastruktur und keine Cyber-Security-Kompromittierung der Grund für deren Probleme. Mit Alarmstufe 3 werden die Kommunikationswege der Rezeptsteuerung zum ERP-System unterbunden und ebenso die restlichen Verbindungen zum Data-Historian. Die Anlage kann wieder angefahren werden und weil das Notfallprotokoll es erfordert, wird nach zwei Stunden eine Neubewertung durchgeführt, die die Zurücknahme der Alarmstufe auf 6 ermöglicht. Damit sind alle Kommunikationswege mit Ausnahme der Fernwartungs-Zugänge auf die Systeme zur Rezeptur-Erstellung und die zum PLS-Engineering wieder offen.

Fazit

Das hier dargestellte Vorgehen hilft als Planungsinstrument für ein geordnetes Vorgehen hinsichtlich der OT-IT-Kommunikation anhand vorzubereitender Tabellen. Deren Inhalt ist naturgemäß abhängig vom betrachteten Betrieb und damit individuell zu erstellen. Durch ein paar Iterationen von Krisenmanagement-Übungen kann die Schlüssigkeit verprobt und das Betriebspersonal geschult werden.

Erwin Kruschitz
anapur AG
67227 Frankenthal

Dr. Walter Speth
Bayer AG
40789 Monheim