# Einleitung

Zur feierlichen Abschaltung des letzten deutschen AKWs sind hochrangige Gäste eingeladen. Unter anderem das BMI und somit Ministerin Schrader. Du, als technischer Sachverständiger und IT-Spezialist darfst die Ministerin begleiten, welche den roten Knopf zur Abschaltung drücken soll. Der AKW-Chef Herr Solar führt Ministerin Schrader, das Fernsehteam und dich durch die Anlage. Nach einigen Minuten gelangt ihr in das Herzstück des AKWs – den Kontrollraum – welches sich hinter einer meterdicken Sicherheitstür befindet.

Ihr begebt euch gemeinsam zum Abschaltterminal. Über ein Mikrofon zählt Herr Solar den Countdown herunter. Die Journalisten außerhalb des Kraftwerks lauschen gespannt mit. Ministerin Schrader hat bereits die Hand auf dem großen roten Knopf. 5...4...3...2……...plötzlich völlige Dunkelheit.

Ihr hört ein lautes Surren und Klicken. Nach einer gefühlten Ewigkeit geht ein rot-pulsierendes Notlicht an und im Kontrollraum verhallt das Warnsignal aus dem Maschinenraum. Die Sicherheitstür wird mit einem Knall verriegelt. Der Bildschirm des Kontrollrechners leuchtet auf und ein Totenkopf erscheint mit folgender Mitteilung:  
"Die Evil Corp hat soeben das Kraftwerk übernommen. Wir haben das Kühlsystem der Brennstäbe gehackt und die Pumpen heruntergefahren.“

Ein Countdown startet: 30:00, 29:59, 29:58, ....

„Zur Entsperrung der Anlage müssen sie nur einen kleinen Betrag von 100.000.000 Dogecoin auf die Wallet-Adresse besser.aBSIchern überweisen."

Unter der Mitteilung erscheint ein Eingabefeld, welches mit Passwort beschriftet ist. Na toll…Ransomware. Der Chef des Kraftwerks ist erschüttert und erklärt, dass es zu einer Kettenreaktion und letzten Endes zur Kernschmelze kommen wird, wenn die Kühlung länger als 30 Minuten stillsteht. Danach fällt er vor Schreck in Ohnmacht. Ministerin Schrader greift sofort zum Telefon um den Kanzler zu fragen, ob die Bezahlung eine Option darstellt. Aber sie hat keinen Empfang. Die Wände des Kontrollraums sind zu dick. Das Fernsehteam steht ratlos in der Ecke des Raumes. Du möchtest nicht warten und glaubst auch nicht, dass eine Bezahlung des Lösegelds wirksam ist. Also suchst du als einziger Anwesender mit breitem IT-Wissen - denn du hast ja DACS studiert ;) - nach einer Lösung.

# Einleitung Raum 1

Du befindest dich nun im Kontrollraum. Die Menge an Schaltern, Hebeln und erschlägt dich fast und es fällt dir schwer deine Panik in den Griff zu bekommen. Du versuchst dich zu sammeln und deine Möglichkeiten abzuwägen:

Du kannst dich im Raum [umschauen]

Du kannst Dinge im Raum [anschauen], [nehmen] und [benutzen]

Du kannst dein aktuelles [Inventar] anschauen

Du kannst dir [Hilfe] suchen, wenn du nicht weiterkommst

## 1. Umschauen Raum 1

Du siehst den Kontrollrechner und Sicherheitsausrüstung in der Ecke.

### Kontrollrechner anschauen

Der Bildschirm zeigt weiterhin den Totenkopf und die Nachricht der Erpresser. Du entdeckst ein Terminal mit Anschlüssen und einigen Knöpfen. Darunter ein Power-Button, ein Reset-Button und eine DIN-AT-Buchse.

#### Power-Button drücken (WENN AN)

Der Rechner fährt herunter.

#### Power-Button drücken (WENN AUS)

Der Rechner fährt wieder hoch, BIOS-Meldungen erscheinen auf dem Bildschirm, ein Windows 95 – Startsound ertönt und die Erpresserbotschaft erscheint direkt wieder nach dem Bootvorgang.

„Das bringt nichts!“, denkst du dir und überlegst, was du tun sollst. Über den Kontrollrechner lassen sich die Pumpen für das Kühlsystem jedenfalls nicht mehr starten. Vielleicht hilft ein manueller Start der Pumpen.

#### Reset-Button drücken

Der Rechner startet neu, BIOS-Meldungen erscheinen auf dem Bildschirm, ein Windows 95 – Startsound ertönt und die Erpresserbotschaft erscheint direkt wieder nach dem Bootvorgang.

„Das bringt nichts!“, denkst du dir und überlegst, was du tun sollst. Über den Kontrollrechner lassen sich die Pumpen für das Kühlsystem jedenfalls nicht mehr starten. Vielleicht hilft ein manueller Start der Pumpen.

#### DIN-AT-Buchse anschauen

So etwas Veraltetes, fast schon Antikes hast du schon lange nicht mehr gesehen. Leider hast du kein Eingabegerät zur Hand, das kompatibel ist.

### Sicherheitsausrüstung anschauen

In der Sicherheitsausrüstung findest du ein Brecheisen.

#### Brecheisen nehmen

„Das könnte eventuell noch nützlich sein“, sagst du und packst das Brecheisen direkt ein.

## 2. Umschauen Raum 1

Du entdeckst die riesige meterdicke Sicherheitstür.

### Sicherheitstür anschauen

Du rüttelst an der Tür, doch sie bewegt sich keinen Zentimeter. Direkt neben der Tür befindet sich ein Tastenfeld und darüber eine Kamera. Du drückst die Grüne Starttaste und die Kamera beginnt mit einem Scan von deinem Gesicht. Du erschrickst. Auf dem Display erscheint in roter Schrift „Zugriff verweigert“. „Das Gesicht des Chefs sollte funktionieren!“, denkst du dir, erinnerst dich aber, dass dieser ohnmächtig geworden ist. Du nimmst dein Smartphone in die Hand und hältst ein Bild von Herrn Solar in die Kamera. „Guten Tag Herr Solar! Bitte geben Sie Ihren PIN ein!“, ertönt eine roboterartige Stimme aus dem Terminal und das Display zeigt: \* \* \* \* \* \*. „Mist, wo krieg ich denn jetzt den PIN her?“, fragst du dich und schaust dich noch einmal um.

## 3. Umschauen Raum 1

Du entdeckst ein Scooter-Poster an der Wand.

### Poster anschauen

Das Poster trägt die Aufschrift „How much is the fish“. Es scheint mit Klebestreifen befestigt worden zu sein. Von der Rückseite schimmert Schrift durch das dünne Papier. Du hebst das Poster an und entdeckst eine Widmung an Herrn Solar mit der Unterschrift von HP Baxxter und einer kurzen Biografie des Künstlers unter anderem mit seinem Geburtsdatum: 16. März 1964

## Mögliche Hilfestellungen

Bei einem Gespräch mit dem Fernsehteam erfährst du, dass der Kraftwerk-Chef totaler Fan von Scooter sei.

# Überleitung Raum 2

Sehr gut. Du konntest die Sicherheitstür öffnen und rennst so schnell du kannst los. Dabei folgst du stur dem Warnsignal, welches dich direkt zum Maschinenraum führt, während es immer lauter wird.

Beim Betreten des Raums nimmst du eine Durchsage einer Computerstimme aus den Lautsprechern wahr: „Noch 20 Minuten bis zur Kernschmelze!“ Die vielen blinkenden Lichter vor Ort werden alle von dem immer noch rot-pulsierenden Licht überdeckt. Das laute Brummen der großen Maschinen ist ohrenbetäubend. Mittig im Raum stehen 5 riesige Pumpen. „Das müssen sie sein!“ Vorsichtshalber ziehst du das Netzwerkkabel des Kontrollrechners des Kühlsystems. Die Hacker dürften jetzt wenigstens keinen Zugriff mehr darauf haben. Was nun?

## Umschauen Raum 2

Du entdeckst die Pumpenventile der riesigen Kühlpumpen und einen Zettel auf einem Tisch in der Nähe. Die Ventile scheinen beschriftet zu sein. Bestimmt muss eine Reihenfolge eingehalten werden.

### Zettel anschauen

Lila – L

Rot – R

Blau – B

Schwarz – S

Grün – G

### Ventile anschauen

Lila Ventil ist mit I beschriftet

Rotes Ventil ist mit II beschriftet

Blaues Ventil ist mit III beschriftet

Schwarzes Ventil ist mit IV beschriftet

Grünes Ventil ist mit V beschriftet

## Richtige Reihenfolge eingegeben

Das muss die richtige Reihenfolge gewesen sein. Doch die Ventile lassen sich nicht drehen. Du brauchst irgendetwas, womit du mehr Kraft aufbringen kannst. Eine Art Hebel.

### Brecheisen benutzen

Die Ventile lassen sich nun drehen. Doch was ist das!? Ein lautes Knarzen übertönt plötzlich das Warnsignal und alle Pumpen gehen wieder aus. Na toll…erneut hörst du eine Durchsage aus den Lautsprechern: „Noch 15 Minuten bis zur Kernschmelze!“

# Überleitung Raum 3

Doch von dem lauten Geräusch scheint der Kraftwerk-Chef wieder aufgewacht zu sein. Er kommt schweren Schrittes auf dich zugelaufen und versucht dir winkend und mit letztem Atem keuchend mitzuteilen, dass die Pumpen nur über den Haupt-Kontrollrechner gestartet werden können.

Du musst also unbedingt einen Weg finden, den Rechner zu entsperren. Doch wie sollst du das bloß anstellen? Vielleicht sind noch nicht alle Rechner mit der Ransomware infiziert. Du musst einen Rechner finden, der noch nicht betroffen ist, vielleicht hilft dir das weiter.

Herr Solar scheint einen Gedankenblitz zu haben: „Wir haben neulich mit anderen Kraftwerken zusammen ein 5G-Campusnetz aufgebaut, das alle verfügbaren Geräte in unserem Netzwerk auflisten kann. Dazu braucht man nur eine passende SIM-Karte. Jedoch hab ich leider vergessen, wo genau die SIM-Karten gelagert werden. Es muss irgendwo hier drüben sein.“, sagt er und führt dich in einen langen, kargen Flur mit sieben Türen.

## Umschauen Raum 3

Auf den Türen entdeckst du seltsame Symbole. Was die wohl zu bedeuten haben? An der Wand hängt außerdem eine Pinnwand und daneben eine Karte von Deutschland.

## Falsche Tür (verschlossen)

Das scheint die falsche Tür zu sein. Leider lässt sie sich nicht öffnen.

## Falsche Tür (offen)

Die Tür ist offen. Du schaust dich im Raum um, doch kannst nichts entdecken, was dir irgendwie weiterhilft. Schade…du hast wertvolle Zeit verloren.

## Richtige Tür

Die Tür ist verschlossen, du siehst allerdings, dass der Schlüssel steckt. Du schließt die Tür auf und betrittst den Raum.

# Überleitung Raum 4

Du scheinst in eine Art Lagerraum gekommen zu sein mit allerlei technischen Geräten, die ihre beste Zeit hinter sich haben. In der Ecke steht ein leeres Serverrack und daneben eine Werkzeugtasche, die allerdings nur nutzlose Werkzeuge enthält. Mal sehen, was du noch so entdecken kannst, was dir weiterhelfen könnte.

## 1. Umschauen Raum 4

An der gegenüberliegenden Wand des Serverracks steht ein Lagerspind mit einem Zahlenschloss, das anscheinend bei der letzten Benutzung nicht richtig verschlossen wurde.

### Spind öffnen

Du öffnest den Spind und schaust dir den Inhalt genau an. Zuerst siehst du nur alte Ersatzteile für Computer. RAM, Lüfter, Netzteile, alte Festplatten und so weiter. Doch dann sticht dir ein kleiner Karton mit der Aufschrift „SIM-Karten“ ins Auge. Du nimmst dir eine Karte aus dem Karton. „Verdammt…wie soll ich denn jetzt den SIM-Slot an meinem Handy öffnen?“, fragst du dich.

Du hörst schnelle Schritte auf dem Gang. Die Ministerin und das Fernsehteam betreten den Raum.

## 2. Umschauen Raum 4

Dir fällt sofort die feine Haarnadel der Ministerin ins Auge. Du fragst sie, ob du dir ihre Haarnadel kurz ausleihen kannst. Sie nickt aufgeregt und übergibt sie dir schnell.

### Haarnadel benutzen

Zum Glück ist die Nadel dünn genug, um den SIM-Slot zu öffnen. Du legst die SIM-Karte in dein Handy ein, worauf die Aufforderung „SIM-PIN eingeben“ angezeigt wird.

## 3. Umschauen Raum 4

An der Innenseite der Spindtür entdeckst du einen QR-Code. Ob der wohl was damit zu tun hat?

### SIM-Pin eingeben

Sehr gut. Du hast es geschafft, die SIM-Karte zu entsperren. Auf deinem Smartphone-Display erscheint direkt das Dashboard der Intranet-Seite des Kraftwerks. In einer Liste am Rand werden alle Computer im Netzwerk angezeigt. Das sieht schlecht aus. Alle PCs sind mit einem Schloss-Symbol versehen. Das kann nichts Gutes bedeuten. Du scrollst durch die Liste. Doch was ist das? Kurz vor Ende der Liste ist tatsächlich noch ein PC aufgeführt, der noch nicht mit einem Schloss-Symbol versehen ist. Das ist es! Du klickst darauf, um dir mehr Details ansehen zu können. Dabei steht sogar eine Raumnummer. „Ich kann Sie dort hinführen!“, sagt der Kraftwerkchef aufgeregt.

# Überleitung Raum 5

Du läufst zusammen mit den anderen zu einer Art Büro-Abteil. Herr Solar geht voran. Ihr betretet ein Büro und schaut euch kurz um. Das Büro ist bestückt mit mehreren Schreibtischen und PC-Arbeitsplätzen. Die meisten von ihnen zeigen die gleiche Nachricht wie der Kontrollrechner und den Totenkopf auf dem Monitor oder sind ausgeschaltet.

## 1. Umschauen Raum 5

Schnell entdeckst du den potentiell nicht betroffenen PC im Raum.

### PC anschauen

Der Bildschirm zeigt ein Anmeldefenster mit einem Passwortfeld. Dir fällt direkt auf, dass auf dem Computer das Betriebssystem Kali Linux installiert ist. Du schaust dich kurz um und entdeckst, dass am Monitor ein Zettel hängt mit der Aufschrift „Passwort“. „Wie blöd!“, denkst du dir, „aber gut für mich!“. Du loggst dich ein und öffnest direkt die Kommandozeile. Mit ein paar Befehlen hast du Zugriff auf den Kontrollrechner bekommen und durchsuchst die Ordnerstruktur nach versteckten Dateien und Verzeichnissen. Nach ein paar Versuchen sticht dir eine Datei ins Auge: encryption\_key\_hash.txt

### Hash-Datei anschauen/öffnen

Die Datei öffnet sich im Text-Editor und darin ist eine Art Code: 781c15abfae7bda64ba65728f73b2b3c

Das muss ein Hash-Wert sein! Welch Ironie, dass auf dem PC Kali installiert ist. Hier muss es irgendwo ein Tool zur Entschlüsselung geben!? Wie ging der Befehl zum Anzeigen von Befehlen noch gleich? Ah genau: list

* Kommandozeile öffnet sich

### Hash-Datei entschlüsselt

Wow. Du hättest nicht gedacht, dass du das hinbekommst, aber du hast tatsächlich das Passwort zur Entschlüsselung des Kontrollrechners gefunden. Jetzt schnell zurück in den Kontrollraum, bevor es zu spät ist.

# Überleitung Raum 6

Ihr seid alle zurück im Kontrollraum angekommen. Du rennst zum Rechner. Verdammt…wo ist die Tastatur? Du findest keine Eingabemöglichkeit. Die Tastaturen der anderen Rechner würden nicht funktionieren. Die sind alle mit USB.

## 1. Umschauen Raum 6

Ihr schaut euch fragend um. Der Kraftwerkchef kommt auf euch zu und fragt nach dem Status. Ihr erläutert ihm kurz das Problem und er zeigt auf eine Wartungsklappe neben dem Kontrollpult. Dort muss eine Tastatur drin sein, die mit dem alten DIN-AT-Anschluss kompatibel ist. Doch die Klappe ist so verrostet, dass du sie mit bloßen Händen nicht aufbekommt.

## 2. Umschauen Raum 6

Im Raum liegt leider nichts mehr herum, das dir weiterhelfen könnte.

## Brecheisen benutzen

Gut, dass du das Brecheisen vom Anfang noch dabei hattest. Du brichst die Klappe auf und dahinter versteckt sich tatsächlich eine Tastatur.

## Tastatur benutzen

Du steckst die Tastatur an den alten Kontrollrechner an und tippst das Passwort ein: 3…0…J…a…h…r…e…B…S…I…1…9…9…1…!

ENTER!

Der Totenkopf verschwindet. Du hast es geschafft. Doch dir fällt etwas ein: „Wir müssen irgendetwas tun, um die Hacker aus dem System zu werfen und das System besser.aBSIchern!“, rufst du. Du wendest dich wieder dem Kontrollrechner zu um dir den Status der Firewall anzuschauen.

## Firewall anschauen

„Ohje…jede Menge Lücken! Wir müssen irgendetwas tun, um die Lücken zu schließen:

* Firewall-ASCII wird mit Lücken angezeigt

## 3. Umschauen Raum 6

In einer Ecke des Kontrollpultes liegt ein Zettel. Vielleicht hilft dir dieser ja weiter.

## Zettel nehmen

ORP.3.A7 | 5

APP.3.4 | 2.2 | 14

ISMS.1.A11 | 4

OPS.1.1.4.A14 | 5

SYS.2.1.A1 | 5

## Satz eingeben/Firewall schließen

Super. Du hast die Angreifer ausgesperrt und die Lücken in der Firewall geschlossen. Ab hier übernimmt der Kraftwerkchef. In letzter Sekunde fährt er über den Kontrollrechner die Pumpen des Kühlsystems wieder hoch. Das rote Notlicht erlischt und das Warnsignal aus dem Maschinenraum ist auch nicht mehr zu hören. GESCHAFFT!