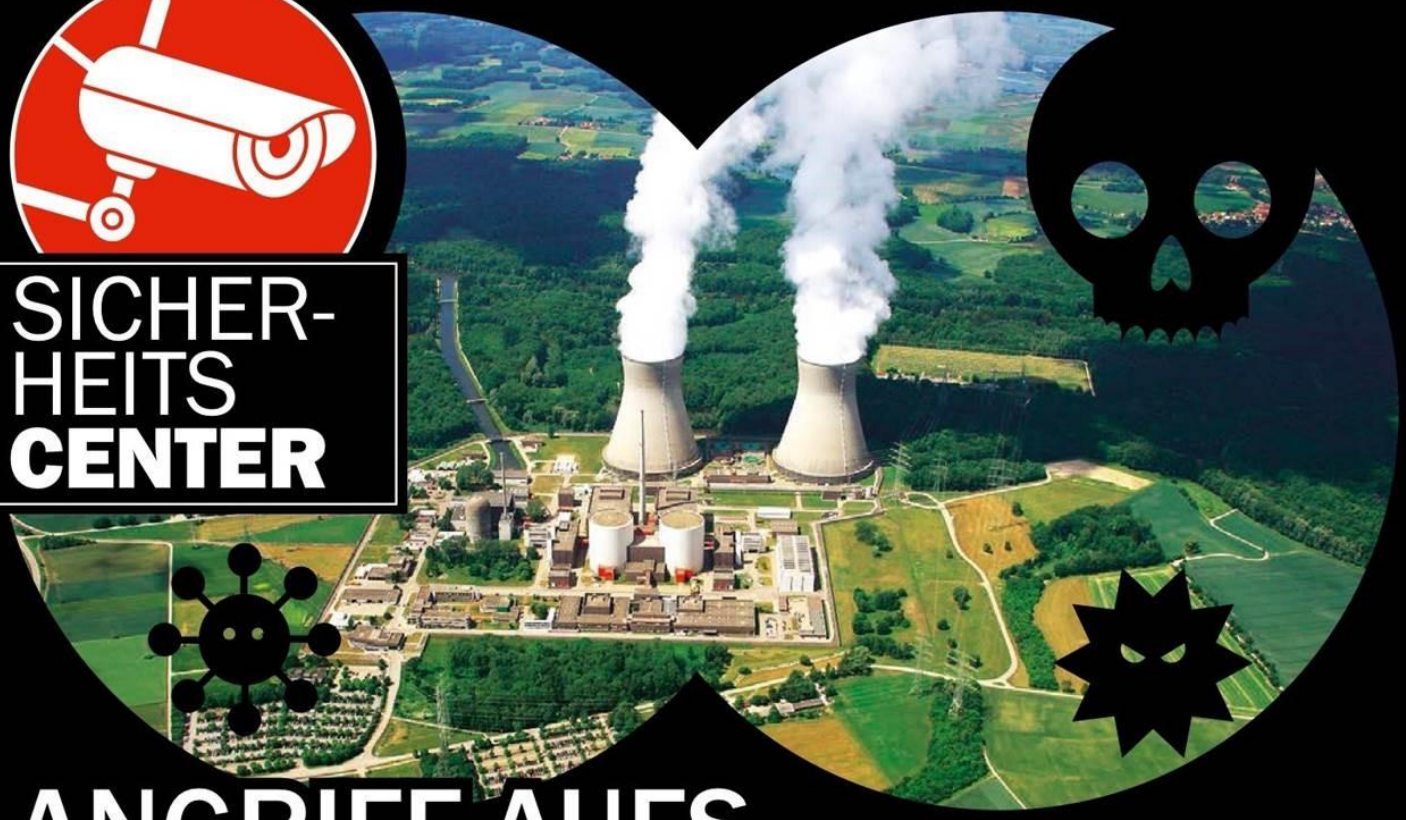
SICHER-
HEITS
CENTER



ANGRIFF AUFS ATOMKRAFTWERK

In Deutschland wurden VIREN in einem ATOMKRAFTWERK entdeckt. COMPUTER BILD hat sich angesehen, wie IT-Teams von gefährdeten Einrichtungen den Ernstfall proben.

Als die Alarmsirene losschrillt, zucken im Kontrollzentrum alle zusammen. Die Telefone gehen aus, die Notbeleuchtung flackert. Das Team sucht hektisch nach dem Fehler, als im Nebenraum heißes Wasser aus einem Druckbehälter schießt. Aber warum zeigen die Kontrollmonitore der Anlage, dass alle Systeme im grünen Bereich sind? Die Mitarbeiter vergleichen Werte, arbeiten Notfallpläne ab, rufen durcheinander. Als Wasserdampf in den Raum eindringt, zieht der Schichtleiter die Notbremse und fährt die Anlage runter. Tausende Haushalte sind ohne Strom. Das Kraftwerk Ritka, 25 Kilometer von Prag entfernt, ist von Hackern komplett lahmgelegt worden.

Dirk Kuchel
Stellv. Chefredakteur

„Terroristen haben Kraftwerke längst im Blick. Deswegen ist es so wichtig, dass die Teams vor Ort vorbereitet sind."

Dies ist (k)eine Übung

Wer bei Google Maps nach dem Kraftwerk sucht, wird es nicht finden – dafür aber ein imposantes Herrenhaus, in dem sich genau dieses Szenario häufiger abspielt. Zu Übungszwecken – damit Attacken auf unsere Infrastruktur keine bösen Folgen haben. Denn die Bedrohung rückt näher: Mitte April gab es im bayrischen Atomkraftwerk Gundremmingen einen unangenehmen Vorfall. Dort waren mehrere Computer von (eher harmlosen) Viren befallen. Auf Ereignisse dieser und weit schlimmerer Art bereitet „CyberGym" vor, Europas erstes „Fitness-Center" für IT-Abteilungen aus kritischer Infrastruktur. Vor allem Betreiber von Atom- und anderen Kraftwerken schicken ihre Teams ins diskrete Herrenhaus nach Tschechien, um sich auf einen Cyberangriff vorzubereiten. Fotos? Tabu, die israelische Firma gibt nur zögerlich ein paar Bilder frei.

Sie kommen!

Die CyberGym-Experten bereiten die Schulungen detailliert vor: Nach dem Legoprinzip bauen die Trainer dazu ganze Industrieanlagen und Unternehmensnetze nach – egal, ob es ein Wasserkraftwerk, eine Raffinerie oder ein Elektrizitätswerk ist. Beim Test soll alles originalgetreu sein, mit echten Steuerbauteilen von Siemens, ABB, Rockwell oder General Electric. Auch Bankennetze oder Kommunikationsverbindungen ausländischer Botschaften bauen die Fachleute mit identischen Managementsystemen, Firewalls und Datenbanken nach. Die Teilnehmer sollen schließlich mit vertrauten Programmen arbeiten.

„Es ist wichtig, alles möglichst nah an der Realität zu haben", erklären die Trainer. Und so ist in Ritka tatsächlich alles echt, sogar der Drucktank mit dem austretenden Dampf. Die Teilnehmer müssen während eines Cyberangriffs unter Zeitdruck Managementreports und Excel-Listen erstellen. In einer echten Krise will der Vorstand ja auch regelmäßig über den aktuellen Stand unterrichtet werden. Die Trainer erzeugen Stress bei ihren Schülern, und das mit Absicht.

Selbst die Mittagspause, die noch auf dem Tagesplan stand, wird während des geprobten Ernstfalls einfach gestrichen. Geplant war sie

ohnehin nie wirklich. Ein Hacker richtet sich schließlich auch nicht nach den Öffnungszeiten der Werkskantine.

Das Training: militärisch präzise

Jeder Raum, jeder Winkel im Trainingszentrum ist kameraüberwacht, die Bilder laufen in einer Kommandozentrale zusammen. Von hier steuert der Übungsleiter die Auftrags-Hacker und beobachtet die Reaktionen des Verteidigungsteams. „Es geht hier nicht darum, möglichst schnell Updates einzuspielen, bevor Hacker eine Lücke ausnutzen können“, erklärt Tomáš Pibyl, der Chef des Trainingszentrums. In einer akuten Gefahrensituation gehe es vielmehr darum, wie eine militärische Einheit zu funktionieren. Er vergleicht das angegriffene Kraftwerk mit einem Verwundeten in der Schlacht. „Man braucht ein Team, das in der Lage ist, unter feindlichem Beschuss den Verwundeten am offenen Herzen zu operieren und am Leben zu halten.“

Israelische Veteranen

Es klingt martialisch, militärische Begriffe sind hier Alltag. Das ist kein Zufall, denn hinter CyberGym Europe stehen Veteranen des israelischen Militärs aus dem Bereich Cyber Defence – also der Abwehr von Angriffen auf Computernetze. Die haben eine Menge Erfahrung mit militärischen Angriffen auf IT-Infrastruktur. Denn längst trainieren Geheimdienste rund um den Globus den Zugriff auf Steueranlagen potenzieller Gegner.

Auch Kraftwerke in Deutschland sind im Visier. Im Ernstfall könnte die Sabotage großer Anlagen für Chaos und Instabilität sorgen. Und auf dunklen Seiten im Internet werden schon seit Langem Sicherheitslücken auch von Kraftwerken regelrecht gehandelt. Die Gefahr solcher Angriffe sorgt bei Experten für weit mehr Sorgen als Vorfälle wie die Gundremmingen-Attacke.

Einsatzbesprechung

Doch zurück nach Ritka bei Prag: Nach jedem Trainingstag findet im Zentrum eine Einsatzbesprechung statt. „Debriefing“ heißt das hier, auch ein militärischer Begriff. Jede Aktion wird bewertet: Was hätte man besser machen können, was lief gut? Das ist wichtig, um die Trainingsangriffe für den nächsten Tag zu planen. Schließlich sollen die Verteidiger mit den Aufgaben wachsen und stressresistenter werden. Um im Ernstfall, der hoffentlich nie eintritt, weniger Fehler zu machen und gut zu reagieren. *[tschö]*

IM TRAININGSZENTRUM

Im tschechischen Ritka werden IT-Teams von Atomkraftwerken auf Hackerangriffe vorbereitet. Einblicke für die Öffentlichkeit gibt es kaum.

HERR IM HAUS

Ein altes Herrenhaus bei Prag beherbergt das CyberGym. Hier wird der Ernstfall geprobt.

EINSATZLEITUNG

Wie reagiert das Team auf Krisen? Die Einsatzleitung beobachtet alle Schritte ganz genau.

REALITÄTSNAH

Der Trainingsraum: Die IT-Teams finden die Geräte vor, die sie auch von ihrer Arbeit kennen.

Foto: AKW Gundremmingen; Montage: COMPUTER BILD