KGG
Kernkraftwerk Gundremmingen GmbH

Meldepflichtiges Ereignis

Gundremmingen, 25.04.2016

Detektion von Büro-Schadsoftware an mehreren Rechnern

Im Kernkraftwerk Gundremmingen ist im Rahmen revisionsvorbereitender Prüfarbeiten in Block B so genannte Büro-Schadsoftware gefunden worden. Diese Software ist in der Fachwelt bereits einige Jahre bekannt; sie zielt unter anderem darauf ab, eine ungewollte Verbindung zum Internet herzustellen.

Die im Kraftwerk an technischen Komponenten eingesetzten Rechner, die für die Steuerung der Anlage genutzt werden, sind nicht mit dem Internet verbunden. Die gefundene Schadsoftware kann zudem keine Veränderungen an technischen Steuerungen bewirken. Alle sensiblen Kraftwerksbereiche sind entkoppelt und grundsätzlich redundant sowie manipulationsgeschützt ausgelegt. Das betroffene IT-System, das 2008 zur Datenverarbeitung und -visualisierung nachgerüstet wurde, gehört zur Brennelement-Lademaschine. Einen Einfluss auf die Steuerung der Lademaschine konnte es aufgrund der Systemarchitektur nicht geben.

Die zuständige Aufsichtsbehörde und das Bundesamt für Sicherheit in der Informationstechnik (BSI) wurden informiert. Die Aufklärung erfolgt mit Unterstützung durch IT-Fachleute des RWE-Konzerns. Im Kraftwerk sind zwischenzeitlich alle weiteren sicherheitstechnisch wichtigen IT-Systeme ohne Befund überprüft worden. Bei einer am 24.04.2016 abgeschlossenen Prüfung von Wechseldatenträgern und Programmiergeräten gefundene Schadsoftware wurde erkannt und bereinigt. Die Vorkehrungen zur IT-Sicherheit sind ausgeweitet worden.

Das Vorkommnis wurde gemäß den deutschen Meldekriterien in die Kategorie N

Rückfragen bitte an
Simone Rusch, T: +49 (8224) 78-3065, F: +49 (8224) 78-83065, E-Mail: presse@kkw.rwe.com

Kernkraftwerk Gundremmingen GmbH, Öffentlichkeitsarbeit, Dr.-August-Weckesser-Str.1, 89355 Gundremmingen

(Normal) eingestuft. Nach der internationalen Skala zur Bewertung von Vorkommnissen (INES) ist es der Stufe 0 zuzuordnen (unterhalb der Skala, keine oder sehr geringe sicherheitstechnische Bedeutung). Eine Gefährdung des Personals, der Umgebung oder der Anlage war damit nicht verbunden.

Aktualisierung 16.12.2016:

Untersuchungen zu Schadsoftware-Fund abgeschlossen – Schutzmaßnahmen optimiert

Die mit Unterstützung von IT-Fachleuten des RWE-Konzerns durchgeführten IT-forensischen Untersuchungen nach einem Fund von Büro-Schadsoftware im April 2016 sind abgeschlossen. Als Konsequenz aus dem Ereignis wurden die Schutzmaßnahmen gegen das Eindringen von Schadsoftware optimiert und massiv verschärft.

Die Erstinfektion mit der Büro-Schadsoftware erfolgte über einen Laptop der Ausbildungsabteilung, der u. a. auch für Präsentationen bei Ausbildungsmessen eingesetzt wurde. Der installierte Virenscanner wurde nicht aktuell gehalten, da das Gerät weder für den Einsatz im Internet vorgesehen, noch mit der Kraftwerks-IT verbunden war. Die Schadsoftware wurde über einen infizierten externen USB-Wechseldatenträger auf den Laptop übertragen.

Im zweiten Schritt wurden zu Ausbildungszwecken Daten zwischen einem Rechner aus dem Werkstattbereich des Betriebsgeländes des Kraftwerks und dem Rechner der Ausbildungsabteilung übertragen. Die Übertragung erfolgte mit Hilfe eines weiteren eingesetzten USB-Wechseldatenträgers. Die Infektion des Visualisierungsrechners der Brennelementlademaschine von Block B erfolgte schließlich über einen weiteren Wechseldatenträger, der zuvor durch den Rechner aus dem Werkstattbereich infiziert worden war. Hierbei wurden existierende Betriebsvorschriften (Virenscan von eingesetzten USB-Wechseldatenträgern) nicht beachtet.

Rückfragen bitte an
Simone Rusch, T: +49 (8224) 78-3065, F: +49 (8224) 78-83065, E-Mail: presse@kkw.rwe.com

Kernkraftwerk Gundremmingen GmbH, Öffentlichkeitsarbeit, Dr.-August-Weckesser-Str.1, 89355 Gundremmingen

Kernkraftwerk Gundremmingen GmbH

Die Sicherheit der Brennelemente-Handhabung war zu keiner Zeit gefährdet. Zur Programmierung von digitalen Steuerungen im Kraftwerk verwendete Rechner haben auch künftig keine Verbindung zum Internet oder zum Firmennetzwerk.

Die für die sichere Reaktorsteuerung verwendeten Systeme sind mit analoger Leittechnik ausgestattet und können durch Schadsoftware generell nicht beeinflusst werden.

Als Konsequenz wurden an allen RWE-Kernkraftwerksstandorten die Schutzmaßnahmen gegen das Einbringen von Schadsoftware noch weiter verschärft. Insbesondere der Zugang mit Rechnern und Wechseldatenträgern zu den Kraftwerken wurde enger reglementiert, der Umgang mit USB-Wechseldatenträgern innerhalb der Kraftwerke völlig neu geregelt. So sind Kraftwerkstechnik und Kraftwerks-IT, gestuft nach der jeweiligen sicherheitstechnischen Bedeutung, nun in Zonen aufgeteilt. In diesen dürfen nur noch neu beschaffte, intern kodierte und system- oder personenbezogene USB-Wechseldatenträger zum Einsatz kommen. Die USB-Wechseldatenträger sind vor Drittzugriff geschützt.

Rückfragen bitte an
Simone Rusch, T: +49 (8224) 78-3065, F: +49 (8224) 78-83065, E-Mail: presse@kkw.rwe.com

Kernkraftwerk Gundremmingen GmbH, Öffentlichkeitsarbeit, Dr.-August-Weckesser-Str.1, 89355 Gundremmingen