Ein Profi-Hacker spricht über Kritische Infrastruktur

Die Schlagzeilen um das Kraftwerk in Weisweiler haben verdeutlicht, dass Kritische Infrastruktur in unserer Region tatsächlich ins Visier geraten kann. Foto: Robin – stock.adobe.com

Der Begriff ist gerade in aller Munde. Einer, der sensible Einrichtungen angreift, ist der Aachener Jens Liebchen. Er ist Auftragshacker.

AACHEN Die Schlagzeilen über das Kraftwerk in Weisweiler haben gezeigt, wie real Anschläge auf Kritische Infrastruktur in unserer Region sind. **Jens Liebchen** kennt sich mit dem Thema bestens aus. Er greift Kraftwerke und sämtliche Infrastruktur digital an, im Auftrag der Eigentümer. Seine 2006 gegründete Redteam Pentesting GmbH sei im Branchenvergleich hoch spezialisiert. Im Interview mit **Carsten Rose** erklärt der 47-Jährige, warum Angreifer immer in der besseren Position sind, dass vieles kritisch ist, was aber nicht als kritisch definiert ist, und die Wirkung von Gesetzen.

Herr Liebchen, wie viele Kraftwerke haben Sie schon gehackt?

Jens Liebchen: Dazu kann ich nichts im Detail sagen, aber es waren Kraftwerke dabei.

Gibt es sicherheitstechnisch Unterschiede bei den verschiedenen Kraftwerken für Sie als Angreifer?

Liebchen: Natürlich. Entscheidend ist, was das Kraftwerk macht und was es im Ernstfall leisten soll. Da unterscheiden sich Kraftwerke deutlich. Manche brauchen Kühlung, andere Brennstoff. Wieder andere sind bei einem Blackout besonders wichtig, weil man sie vergleichsweise einfach und manuell wieder hochfahren könnte. Insofern unterscheiden sich auch die Angriffe.

Was hacken Sie genau?

Liebchen: Typischerweise starten wir an einem vereinbarten Punkt. Das kann bedeuten, dass ein bestimmter Rechner im Netzwerk bereits kompromittiert wurde. Von dort aus versuchen wir, in Richtung Kraftwerksteuerung vorzudringen – also dorthin, wohin man normalerweise nicht gelangen sollte. Es kann aber auch um ganz andere Szenarien gehen. Das hängt stark davon ab, was für den Kunden sinnvoll ist und welches Ziel wir erreichen sollen.

Würden Sie bei der Sicherheit von Kraftwerken priorisieren? Unterscheiden sich im Ernstfall Wasser- von Atomkraftwerken?

Liebchen: So allgemein kann man das nicht sagen, aber es gibt Situationen, in denen genau das gilt. Ein Beispiel ist der komplette Blackout: Alle Kraftwerke sind heruntergefahren, weil die Netzstabilität nicht gesichert werden konnte. Dann muss man das System wieder anfahren. Dafür braucht man Strom – und der muss irgendwoher kommen. Entweder lässt er sich importieren. Oder aber es kann sein, dass sich die Netze entkoppelt haben, damit andere Länder weiter Strom haben, während wir im Dunkeln stehen. Dann sind gerade Wasserkraftwerke interessant. Sie lassen sich vergleichsweise gut manuell in Betrieb nehmen – etwa indem man ein Ventil öffnet, den ersten Strom erzeugt und danach Schritt für Schritt größere Kraftwerke startet.

Zerstören Sie bei Ihren Tests auch Infrastruktur und Systeme?

Liebchen: Zerstörung versuchen wir natürlich zu vermeiden. Aber wir wollen sichtbar machen, was möglich ist. Bei einem Kraftwerk gibt es etwa Stromzangen, die sich bewegen können. Die bewegen wir nicht selbstständig, dafür ist ein Techniker dabei. Wenn wir aber zeigen wollen, dass wir aus einem bestimmten Netzwerk heraus auf die Steuerung zugreifen können, bekommen wir dafür das Okay. Dann können wir eine solche Stromzange öffnen oder schließen – und man sieht physisch, was digital möglich geworden ist.

Sie haben sicher weitere solcher Beispiele.

Liebchen: Bei einem Flughafen ist die Anflugbefeuerung auf der Start- und Landebahn ein gutes Beispiel: Man kann Lichter an- oder ausschalten. Dadurch wird allen Beteiligten

bewusst, was es bedeutet, wenn jemand, der relativ weit außen startet, plötzlich auf sehr Kritische Systeme zugreifen kann. Dafür braucht man gute Szenarien. Dabei helfen unsere Kunden mit, damit klar wird, was das Risiko in der Praxis bedeutet. Dann kann man nach vorne schauen, statt darüber zu diskutieren, ob das Gefundene überhaupt eine Schwachstelle ist.

Es klingt, als könnten Sie wirklich alles umsetzen, was sich ein Angreifer ausdenken kann.

Liebchen: Ganz so wie im Film ist es vielleicht nicht. In der Praxis erzielen wir aber relativ häufig Erfolge. Dann sprechen wir über Fakten. Wir sind froh, wenn anschließend Maßnahmen getroffen werden – auch solche, die unpopulär sind, weil sie teuer oder aufwendig sind. Wenn Kunden uns später zurückmelden, dass wir sie ein großes Stück weitergebracht haben, weil sie Lücken schließen konnten, die sie ohne uns nie entdeckt hätten, ist das genau das Ziel.

Was definieren Sie als Kritische Infrastruktur?

Liebchen: Das ist schwer zu sagen. Der Begriff stammt aus verschiedenen Bereichen: aus dem Kritis-Gesetz (*Anm. d. Red.: Dachgesetz zur Stärkung der physischen Resilienz Kritischer Anlagen*), aber auch vom Bundesamt für Bevölkerungsschutz, das eine etwas andere Definition hat. Kritische Infrastruktur ist grundsätzlich das, was für viele Menschen besondere Bedeutung hat. Die Schwelle liegt bei 500.000 Menschen. Aber auch vieles, woran man zunächst nicht denkt, kann Kritische Infrastruktur sein – etwa die Müllabfuhr. Wenn der Müll lange liegen bleibt, ist das weder gesund noch gut. Für uns macht es in der Praxis aber keinen riesigen Unterschied, ob wir eine Kritische Infrastruktur angreifen oder eine andere gut geschützte Infrastruktur mit weniger Betroffenen. Wichtig ist, dass die Verantwortlichen eine eigene Motivation haben, das Sicherheitsniveau hochzuhalten. Dann unterscheiden sich Kritische und nicht Kritische Infrastrukturen vor allem darin, ob es verpflichtende Meldewege gibt. Die Maßnahmen selbst sind ähnlich oder gleich.

Wie lässt sich Kritische Infrastruktur – auch solche, die erst auf den zweiten Blick kritisch ist – besser schützen?

Liebchen: Die Frage ist, ob wir das als Gesellschaft immer wollen, denn hundertprozentige Sicherheit wird es nie geben. Außerdem ist alles ein Gesamtsystem. Egal, wie gut einzelne Teile geschützt sind: Der Angreifer hat einen großen Vorteil. Er sucht sich die schwächste Stelle; der Verteidiger dagegen muss überall aufrüsten. Deshalb ist es schwierig zu sagen: Ich schütze alle Systeme so, dass niemand mehr durchkommt. Entscheidend ist der nächste Schritt: Was passiert, wenn jemand durchkommt? Kann ich verhindern, dass sich ein Angriff von einem PC auf das gesamte Netzwerk ausbreitet? Und wenn er sich ausbreitet: Habe ich ein Backup, um das System

wieder hochfahren zu können? An verschiedenen Stellen muss man Hürden setzen, um Angreifer zumindest zu entdecken – und möglichst auch aufzuhalten.

Welche Rolle spielt für Sie die Politik? Sie macht die Gesetze und legt Verantwortlichkeiten fest – was bei Kritischer Infrastruktur nicht immer leicht zu durchschauen ist.

Liebchen: Ich weiß nicht, wie groß die Rolle in der Praxis tatsächlich ist. Es ist schwer zu sagen, was wäre, wenn es das Kritis-Gesetz nicht gäbe. Würden die Unternehmen deshalb wesentlich schlechter arbeiten? Das ist hypothetisch. Ich sehe auch Bereiche, die nicht unter das Kritis-Gesetz fallen und trotzdem eine angemessene Absicherung betreiben, obwohl sie dazu nicht verpflichtet sind. Was wir allerdings sehen: Wenn wir in Bereichen testen, in denen Bevölkerungsschutz eine große Rolle spielt, sitzen am Ende im Abschlussgespräch auch andere Beteiligte wie Politiker mit am Tisch. Die können ihre nächsten Entscheidungen von unseren Ergebnissen abhängig machen.

Haben Sie mit Ihrer Arbeit mal eine Katastrophe verhindert?

Liebchen: Das wissen wir leider nicht. Ich gehe davon aus, dass wir in vielen Fällen dazu beigetragen haben, Systeme sicherer zu machen. Deshalb sind manche Dinge vielleicht gar nicht erst passiert. Aber darüber zu sprechen, was nicht passiert ist, weil wir gearbeitet haben, bleibt hypothetisch. Unsere Kunden sagen jedenfalls, dass wir sie weiterbringen. Insofern werden wir sicherlich das eine oder andere verhindert haben.