

Datenklau und Virenstreuungen waren gestern: Längst können Kriminelle über computergesteuerte vernetzte Anlagen die Produktion manipulieren

Von Katja Wilke

Wer Lebensmittel herstellt, lernt, mit Drohbriefen zu leben. Ein unbeobachteter Moment, schon steht das vergiftete Produkt im Regal. An die Erpresserbriefe gewöhnt man sich niemals – aber man weiß, was kommt. Umso überraschter war der Geschäftsführer eines Unternehmens, dem ein Brief mit einer ungeahnten kriminellen Qualität auf den Tisch flatterte. Die Verfasser verkündeten, sie hätten sich über Fernwartungszugänge in die zentrale Steuerung der Produktionsmaschinen eingeklinkt. Nun könnten sie nach Lust und Laune die Temperatur, mit der Maschinen die wärmeempfindlichen Lebensmittel verarbeiteten, ändern. Der Clou: Die Manipulation wäre nicht zu entdecken, denn die Erpresser konnten auf die Displays zugreifen und dadurch eine gleichbleibende Temperatur anzeigen lassen.

Kein ausgedachtes Beispiel, auch wenn Jyn Schultze-Melling den Namen des Unternehmens nicht preisgibt. Der auf Informationstechnologie (IT) spezialisierte Anwalt der Kanzlei Nörr Stiefenhofer Lutz sagt: „Derartige Fälle zeigen, wie anfällig breitbandig vernetzte Industrieanlagen sind.“ Auch wenn in diesem Fall keine Kunden gefährdet waren, weil die Produktion umgeleitet wurde – und die Täter gefasst werden konnten.

Die IT als Einfallstor für Kriminelle ist längst Alltag in deutschen Unternehmen. Das Bewusstsein für diese Gefahr ist aber nach wie vor, wenn überhaupt, nur latent vorhanden. „Viele Unternehmen vernachlässigen ihre Sicherheit an den entscheidenden Stellen“, sagt Sebastian Schreiber, Geschäftsführer der IT-Beratung SysS. Schreiber testet als sogenannter White-Hat-Hacker, also als Auftrags hacker, die Computersysteme von Konzernen und Mittelständlern. „Häufig genügt müssen Unternehmen erst Opfer eines Angriffs werden, bevor sie die Sicherheit ihrer Netzwerke auf den neuesten Stand bringen.“

Treffen kann solch ein Angriff jeden. „Wirtschaftskriminalität ist keine Frage der Unternehmensgröße. Gerade kleinere bis mittlere

Mittelständler denken häufig, dass sie uninteressant für Kriminelle sind“, sagt Felix Juhl, Geschäftsführer der Gesellschaft für technische Sonderlösungen. Falsch, meint Juhl: „Insbesondere innovative und hoch spezialisierte kleinere Unternehmen müssen Onlineattacken von Hackern, Wirtschaftsspionen und Kriminellen fürchten.“

Bislang fürchten sich Firmenchefs in erster Linie vor eingeschleusten Viren und vor heimlichem Datenklau – etwa der Lieferantenlisten oder Geschäftszahlen. Die neue Qualität der Computerkriminalität ist ihnen selten bewusst.

Insbesondere bei produzierenden Unternehmen haben Hacker oft leichtes Spiel. Die Standardisierung in der Automatisierungstechnik verlagert die Problematik zunehmend von den Büros in die Welt der Fertigung – wo sie viele Unternehmen unvorbereitet trifft.

Verwendet ein Betrieb beispielsweise weltweit vertriebene Steuerungssysteme, kennen Kriminelle deren Schwachstellen häufig genau. In der Regel werden diese Systeme in einer Konfiguration verkauft, die vom Nutzer nicht geändert werden darf – ansonsten verfällt die Herstellergarantie.

Individuell konfigurierte Software ist nicht unbedingt sicherer. So sind Steuerungssysteme vor allem im Maschinen- und Anlagenbau häufig bunt zusammengewürfelt und veraltet. Externe können sich leicht Zugriff auf die gesamten Produktionsabläufe verschaffen, weil die Produktion heute – selbst wenn sie über mehrere Standorte läuft – zentral gesteuert wird. Das führt dazu, dass alle Maschinen vernetzt und deshalb besonders anfällig für Angriffe sind.

Die Crux für Unternehmen: Je effizienter sie ihre Abläufe gestalten, desto anfälliger werden sie. „Dieses unkalkulierbare Risiko kompensiert die erhoffte Effizienz der Vernetzung“, warnt Schultze-Melling.

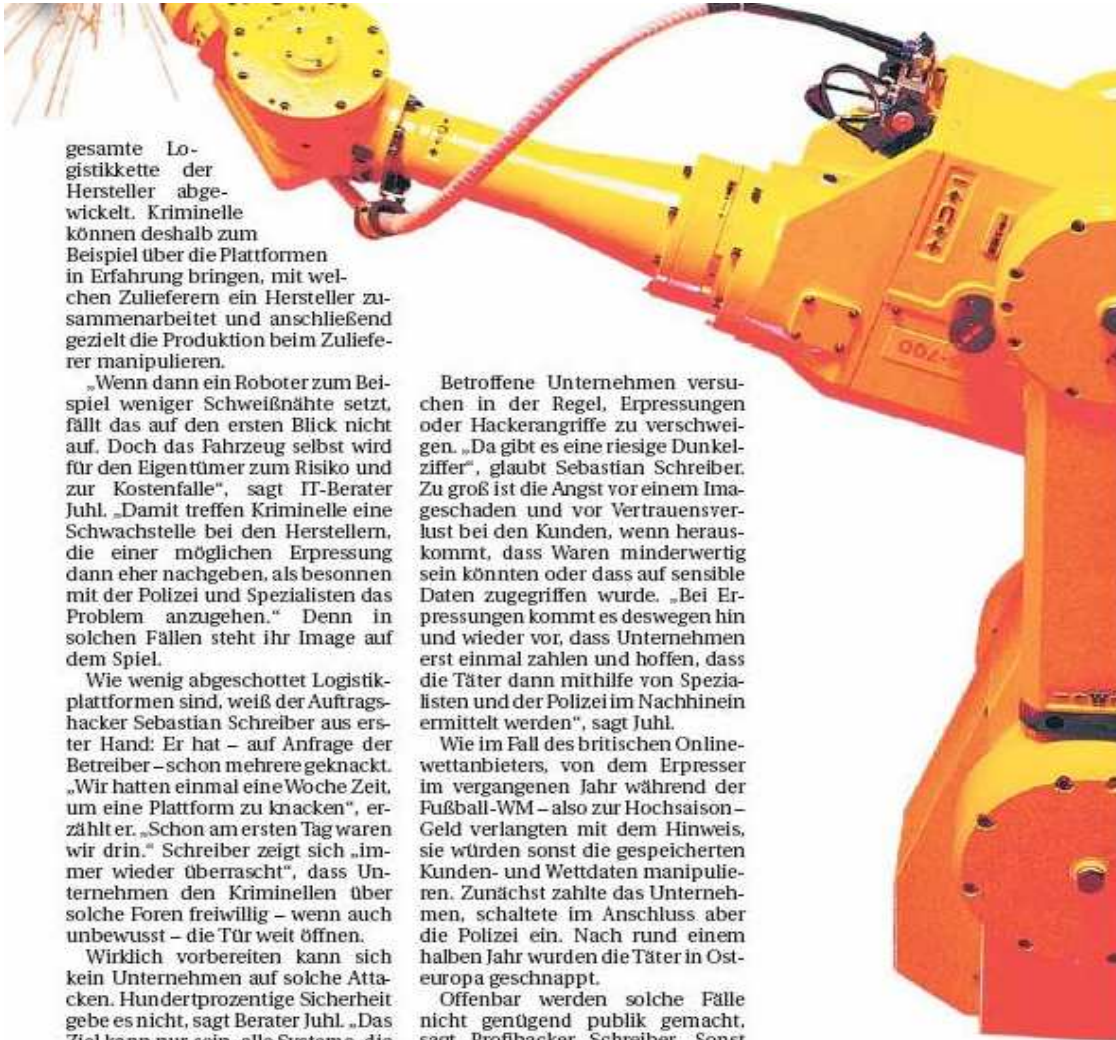
Wenn organisierte Banden einen Konzern erpressen oder missgünstige Wettbewerber ihm schaden wollen, aber keine direkten Angriffspunkte finden, suchen sie gern bei Zulieferern nach Schwachstellen. Anfällig ist dabei insbesondere die Automobilbranche.

Statt wie früher mit Zulieferern langfristig zusammenzuarbeiten, schreiben die Hersteller die Teile, die sie benötigen, heute in der Regel auf speziellen Branchenplattformen aus. Auf diesen Plattformen wird die



Die Prozesse in der Nahrungsmittelindustrie und im Autobau werden verstärkt vom **Computer gesteuert**. Aber wer steuert den Computer?





gesamte Logistikette der Hersteller abgewickelt. Kriminelle können deshalb zum Beispiel über die Plattformen in Erfahrung bringen, mit welchen Zulieferern ein Hersteller zusammenarbeitet und anschließend gezielt die Produktion beim Zulieferer manipulieren.

„Wenn dann ein Roboter zum Beispiel weniger Schweißnähte setzt, fällt das auf den ersten Blick nicht auf. Doch das Fahrzeug selbst wird für den Eigentümer zum Risiko und zur Kostenfalle“, sagt IT-Berater Juhl. „Damit treffen Kriminelle eine Schwachstelle bei den Herstellern, die einer möglichen Erpressung dann eher nachgeben, als besonnen mit der Polizei und Spezialisten das Problem anzugehen.“ Denn in solchen Fällen steht ihr Image auf dem Spiel.

Wie wenig abgeschottet Logistikplattformen sind, weiß der Auftrags-hacker Sebastian Schreiber aus erster Hand: Er hat – auf Anfrage der Betreiber – schon mehrere geknackt. „Wir hatten einmal eine Woche Zeit, um eine Plattform zu knacken“, erzählt er. „Schon am ersten Tag waren wir drin.“ Schreiber zeigt sich „immer wieder überrascht“, dass Unternehmen den Kriminellen über solche Foren freiwillig – wenn auch unbewusst – die Tür weit öffnen.

Wirklich vorbereiten kann sich kein Unternehmen auf solche Attacken. Hundertprozentige Sicherheit gebe es nicht, sagt Berater Juhl. „Das Ziel kann nur sein, alle Systeme, die vernetzt sind, so sicher wie möglich zu machen.“ Fest steht: Je mehr Firmen Zugriff haben, desto gefährlicher wird die Vernetzung.

Nicht immer stehen Kriminelle hinter den Attacken. Ebenso anschaulich wie abschreckend wirkt der Fall eines Zulieferers, der einen Testvirus auf seinem System laufen ließ, um die Sicherheit der eigenen PC zu testen. Unglücklicherweise gelang es ihm nicht, das Virus unter Kontrolle zu halten, und es gelangte über die Plattform in das Computernetz eines in Deutschland produzierenden Autoherstellers. Zwei Tage lang standen durch das Virus beim Hersteller die Bänder still – und führten zu entsprechenden Lieferverzögerungen.

Betroffene Unternehmen versuchen in der Regel, Erpressungen oder Hackerangriffe zu verschweigen. „Da gibt es eine riesige Dunkelziffer“, glaubt Sebastian Schreiber. Zu groß ist die Angst vor einem Imageschaden und vor Vertrauensverlust bei den Kunden, wenn herauskommt, dass Waren minderwertig sein könnten oder dass auf sensible Daten zugegriffen wurde. „Bei Erpressungen kommt es deswegen hin und wieder vor, dass Unternehmen erst einmal zahlen und hoffen, dass die Täter dann mithilfe von Spezialisten und der Polizei im Nachhinein ermittelt werden“, sagt Juhl.

Wie im Fall des britischen Online-wettanbieters, von dem Erpresser im vergangenen Jahr während der Fußball-WM – also zur Hochsaison-Geld verlangten mit dem Hinweis, sie würden sonst die gespeicherten Kunden- und Wettdaten manipulieren. Zunächst zahlte das Unternehmen, schaltete im Anschluss aber die Polizei ein. Nach rund einem halben Jahr wurden die Täter in Osteuropa geschnappt.

Offenbar werden solche Fälle nicht genügend publik gemacht, sagt Profihacker Schreiber. Sonst würden sich Unternehmen doch intensiver um die Sicherheit ihrer IT kümmern. Schreiber glaubt, dass Chefs oftmals gar nicht erfahren, wie schlecht es um ihre Firewalls und die Virenabwehr bestellt ist. „Wenn Systemadministratoren oder IT-Manager durch uns von früheren Angriffen auf ihr System erfahren, reichen sie dieses Wissen nicht unbedingt an ihre Vorgesetzten weiter“, sagt Schreiber. „Andernfalls müssten sie sich unangenehmen Fragen aussetzen.“

Für Vorstände und Geschäftsführer wäre dieses Wissen allerdings sehr wichtig. Wenn eigene Sicherheitslücken in der IT anderen Firmen einen Schaden zufügen, steht das eigene Unternehmen in

der Haftung. Zudem haften die Manager auch persönlich gegenüber ihrem Unternehmen, wenn ein Schaden entsteht – wenn also die Produktion angehalten werden muss oder wichtige Daten unwiederbringlich verloren gehen.

Niedergelegt ist diese Haftung in den Bußgeldvorschriften aus dem Bundesdatenschutzgesetz und auch im Paragraf 93 des Aktiengesetzes, der die Sorgfaltspflicht von Vorständen regelt. Diese Pflicht sollten Manager ernst nehmen, sagt Anwalt Schultze-Melling, „denn die persönliche Haftung kann unter Umständen schnell existenzbedrohende Ausmaße annehmen“.