Ladung schützen

Ortung: Trakalog ist der Name eines Sicherungssystems für Container. Es protokolliert sämtliche Bewegungen, Standorte und Türöffnungen auf dem Transportweg.

Fotos: ISS

Langfingern keine Chance: Trakalog kommt ohne Schalter aus. Das soll Manipulationen ausschließen.

Es sind Aussagen, wie die von Heiner Jerofsky, die hellhörig machen: »Internationale Diebesbanden verursachen laut einer EU-Studie jährlich neun Milliarden Euro Schaden in europäischen Transportketten«, sagt der Kriminalrat im Ruhestand. Die Dunkelziffer dürfte indes noch höher sein, denn über Diebstahl in der Transportbranche spricht eigentlich keiner. Meist stecke organisierte Kriminalität hinter den Diebstählen. Das Gros der Täter ist gut organisiert und informiert. »Gestohlene Waren geht sofort weg«, erklärt Jerofsky.

Er rät Unternehmen zum einen, Fahrer und Subunternehmer gründlich auszuwählen. Und wer die Mittel hat, sollte darüber hinaus in Überwachungs- und Sicherungstechnik investieren. Das klappt im Speditionslager recht unkompliziert, schwieriger wird es, wenn die Ware auf dem Lkw ist. Doch auch hier gibt es Lösungen, beispielsweise das Container-Sicherungs-und Überwachungssystem Trakalok vom britischen Hersteller Loksys. In Kürze bringt das Unternehmen ein Sicherungssystem für Wechselbrücken auf den Markt. »Es hat lange gedauert, aber jetzt gibt es einen Prototyp für Wechselbrücken mit Rolltoren«, erklärt Gunnar Druskat, Geschäftsführer von Industrial Supply Service (ISS). Von Mölln aus vertreibt ISS seit zwei Jahren Trakalok in Deutschland.

> Das Gros der Täter ist gut organisiert

Doch was unterscheidet das britische Produkt von anderen? Schließlich gibt es bereits für weniger als 35 Euro Geräte aus chinesischer Produktion mit GPS-Funktion.

Von diesen Geräten hält Druskat nichts. »Wir wollen nicht nur wissen, wo der Container ist. Wir wollen auch informiert werden, wenn an der Tür manipuliert wird«, sagt er. Wenn dann am Ende der Reise tatsächlich etwas fehlt, kann anhand des erstellten Protokolls genau festgestellt, wo und wann manipuliert wurde. Damit lässt sich der Schaden demjenigen zuordnen, der für diesen Zeitraum haftet. »Das ist ein ganz wichtiger Aspekt«, betont Druskat.

Das System protokolliert also sämtliche Bewegungen, Standorte und Türöffnungen des Containers. »Wir können auch im Vorfeld festlegen, welche Routen der Container nehmen soll und ob es Gefahrenzonen gibt, die der Fahrer unbedingt meiden soll«, so Druskat. Trakalok kann sich aber auch dann melden, wenn bestimmte Wegpunkte erreicht sind. Es können sichere Zonen definiert werden, in denen Türöffnungen zwar protokolliert, aber keine Benachrichtigungen versendet werden. Dagegen meldet sich das Gerät immer, wenn der Batteriezustand kritisch ist.

Auf den ersten Blick sieht Trakalok ziemlich unspektakulär aus. Es besteht aus einem Metallgehäuse, das eine Telematik-Einheit schützt. »Am Gerät selbst sind keine Schalter«, betont Druskat. Das Gerät wird von außen am Verschlusshebel der linken Schließstange der rechten Tür angebracht. Bei internationalen Transporten sichert das Zollsiegel auch Trakalok. Das Gehäuse verdeckt mehrere Befestigungspunkte des Türverschlusses des Containers und schützt so vor Manipulation.

Trakalog aktiviert sich automatisch, wenn es an einem Container angebracht wird. Die Betriebsbereitschaft zeigen LED-Lampen an. Bei fehlender Montage am Container sendet die Einheit eine Meldung an das System. Sollte der Zoll den Inhalt des Containers überprüfen wollen, öffnet er das angebrachte Siegel, verschiebt den Bolzen und kann dann die Tür öffnen. »Der Zoll wird in den Frachtpapieren vermerken, dass der Container geöffnet und mit einem neuen Siegel versehen wurde«, sagt Druskat. Anhand des Protokolls lassen sich diese gewollten Öffnungen dann zuordnen.

Manipulationen lassen sich entweder in Echtzeit melden. Kann das System die Position aktuell nicht berechnen, beispielsweise wenn es unter Deck an Bord eines Seeschiffs gelagert ist, meldet es sich erst, wenn es wieder ein Netz hat. »Wir sind darauf angewiesen, welches Netz gerade vorhanden ist«, sagt Druskat. Die Datenübertragung erfolgt über GPRS oder GSM. Informiert wird per Sprachnachricht, SMS, E-Mail oder einer Kombination aus allen. Druskat garantiert die Funktionsfähigkeit von Trakalog bis zu Temperaturen von minus 24 Grad.

Verwaltet wird das Gerät und seine Daten über eine Webplattform. Dort können alle Parameter im Betrieb geändert werden. Die Daten können unabhängig vom Format an Kundensysteme überspielt werden. Im Einsatz ist Trakalog bei DHL sowie Kühne + Nagel »Jede Einheit kostet weniger als 200 US-Dollar im Monat«, erklärt Druskat. Nicht sein viel viel, wenn man bedenke, dass ein mit Zigaretten gefüllter 40 Fuß-Container – verzollt – eine Million Euro wert ist.

Um die ständig steigende Nachfrage besser koordinieren zu können, passt Loksys momentan die internen Strukturen an. »Wir bauen gerade an einem weltweiten Netzwerk«, sagt Druskat. Denn nicht jedes Unternehmen kann sich um den Rücklauf der Trakalog-Einheiten kümmern.

Schon werden die ersten Versicherungen hellhörig. »Der Wunsch nach 100-prozentiger Integrität der Ladung wird größer«, erklärt Druskat. Mögliche Rabatte mit den Versicherungen auszuhandeln, sei dann aber letztlich Sache des Dienstleisters.

Annett Boblenz

DER ANBIETER

ISS Industrial Supply Service ist ein Handelshaus. Vom Firmensitz in Mölln in Schleswig-Holstein, einer Niederlassung in Indonesien und Repräsentanten in Thailand, Malaysia, den Philipinen sowie Süd-China betreut das Unternehmen Geschäftspartner in Mittel- und Fernost.

Mit Sicherheit gefährdet

Spionage: Eine Analyse der Sicherheitsexperten von Mandiant zeigt, wie weit Hackerangriffe gehen. Die Logistikbranche gehört dabei zu den beliebtesten Zielen.

Auf dem Reich der Mitte liegt ein Schatten. Und zwar nicht erst, seit die US-amerikanische Sicherheitsfirma Mandiant im Februar einen Bericht zur Sicherheit der Daten im Internet vorlegte. Laut dieser Analyse befindet sich China im Cyber-Krieg. So ist in dem Bericht zu lesen, dass es bei der Volksbefreiungsarmee eine spezielle Elitetruppe namens 61398 gibt, die aus Hackern besteht.

Wem das zu weit weg scheint, den sollten zwei Fakten aufrütteln: Zum einen gehört das Transportgewerbe zu den bevorzugten Zielen der Internetkriminellen (siehe Kasten). Zum anderen konstatieren auch die deutschen Bundesbehörden eine zunehmende Gefahr durch Cyber-Angriffe aus China. Mehr als 1.000 IT-Angriffe auf Unternehmen in Deutschland soll es allein im vergangenen Jahr gegeben haben.

Die Einfallstore sind laut Bundesamt für Sicherheit in der Informationstechnik (BSI) denkbar einfach. Zwar verlieren die Sicherheitslücken des Betriebssystems wie etwa Microsoft Windows zunehmend an Bedeutung. Dafür bieten die Anwendungen aber genügend Angriffsfläche.

Der Browser, also das Programm, mit dem der PC-Nutzer ins Internet geht, ist eine mögliche Schwachstelle. Der Webbrowser Mozilla Firefox liegt in Europa bezüglich des Marktanteils mittlerweile an der Spitze. Er wies wie laut BSI im Jahr 2010 rund 107 Schwachstellen auf, davon eröffneten 60 die Möglichkeit eines Cyber-Angriffs.

Auch der sogenannte Adobe Flash Player, der nach Herstellerangaben auf mehr als 99 Prozent aller PCs in Europa läuft, ist ein dankbares Ziel für Angriffe. Der bot 2010 laut BSI 60 Schwachstellen, von denen 53 zum Ausführen von Schadcodes ausgenutzt werden konnten. Und: Je mehr Anwendungen auf einem PC laufen, desto mehr potenzielle Einfallmöglichkeiten für Hacker gibt es.

Aber nicht nur Anwendungen, die in direktem Zusammenhang mit der Internetnutzung stehen, sind unter Umständen gefährlich. So berichtet das BSI dass beispielsweise im Februar 2011 mehr als 20 Lücken in Microsoft-Produkten, darunter auch Office, bekannt waren. Immerhin 16 davon stellten eine ernsthafte Gefahr dar.

Das Fazit des BSI ist da nicht gerade beruhigend: »Die Bedrohung durch Schwachstellen in Software-Produkten befindet sich auf einem sehr hohen Niveau und steigt weiter. Diese Situation wird verschärft durch lange Zeiträume, in denen keine Patches für öffentlich bekannte und teilweise kritische Schwachstellen verfügbar sind.«

Problematisch sind natürlich auch Schadprogramme wie Viren, Trojaner oder Würmer, die nicht immer von den Schutzprogrammen entdeckt werden. Gerade beim Surfen im Internet sei es daher ratsam, mit sogenannten Virtualisierungstechniken zu arbeiten. Soll heißen, dass auf dem PC eine virtuelle Arbeitsoberfläche geöffnet wird und der Nutzer von dort aus mit dem Browser ins Internet geht. So lasse sich zumindest Datenverlust und Sabotage ausschalten.

Wo wir wieder zurück im Unternehmen selbst wären: Da muss es in kleineren Unternehmen nicht unbedingt der eigens dafür eingeschleuste Wirtschaftsspion sein. Da reicht auch schon ein enttäuschter Ex-Mitarbeiter. Viele glauben auch, die eigenen Angestellten seien über jeden Zweifel erhaben. Dazu meinen die BSI-Experten: »Die Mehrzahl der Sicherheitsverstöße wird durch Innentäter verursacht. Dabei muss nicht immer Vorsatz im Spiel sein. Auch durch Versehen, Übereifer oder Neugierde gepaart mit mangelndem Problembewusstsein entstehen manch mal große Schäden.« Also der allzu sorglose Umgang mit Unternehmensdaten, die auf ungesicherten Datenträgern oder Geräten aus der Firma herausgetragen werden.

Und wer glaubt, dass sein Unternehmen für derartige Angriffe doch viel zu uninteressant ist, sollte Folgendes Bedenken: Ähnlich wie bei Schwerpunktstreiks in der Industrie, reicht es natürlich auch, ein kleines, aber entscheidendes Rädchen in der Wertschöpfungskette auszuschalten. Wenn eine Just-in-time-Belieferung scheitert, dann steht das Band still. Da muss es nicht der viel beschworene chinesische Spion sein.

Carsten Nallinger

AUSGEWÄHLTE HACKER-ZIELE

- IT-Branche: 19
- Luft und Raumfahrt:16
- Behörden: 12
- Satelliten, Telekommunikation: 12
- Forschung/Beratung: 10
- Energie: 8
- Transport: 8
- Bau und Industrie: 7

Bei insgesamt 141 nachgewiesenen Cyber-Attacken.

Quelle: Mandiant

Foto: Fotolia

Die Gefahr droht nicht nur durch Wirtschaftsspione aus China. Oft ist es einfach Sorglosigkeit.