INNOVATIONSPREIS DER WIRTSCHAFTSZEITUNG 2017

Ideen gesucht

OSTBAYERN. Bereits zum siebten Mal schreibt die Wirtschaftszeitung 2017 den Innovationspreis aus. Die Carolinenhütte GmbH & Co. KG, die Maschinenfabrik Reinhausen, die PCO AG, die Sturm Blechverarbeitung & Systeme GmbH, die Osram Opto Semiconductors GmbH sowie die Krones AG waren die bisherigen Preisträger. Wer sich für den siebten Innovationspreis bewerben möchte, kann seine innovative Geschäftsidee kurz in einer Mail skizzieren und an innovationspreis@ die-wirtschaftszeitung.de schicken.

Nominiert für den Innovationspreis: DS Deutsche Systemhaus GmbH

Da beißen Hacker sich die Zähne aus

Die DS Deutsche Systemhaus GmbH in Schwandorf und die österreichische Blue Shield Security GmbH bringen eine revolutionäre IT-Sicherheitslösung auf den Markt.

Von Theo Kurtz

SCHWANDORF. Es kann einem himmelangst werden, wenn man Christian Paulus, dem Geschäftsführer der Deutsche Systemhaus GmbH in Schwandorf, zuhört. Schlaue, aber kriminelle Köpfe treiben in den schier endlosen Weiten des World Wide Web ihr Unwesen, legen Computer lahm, spionieren Unternehmen aus und richten dabei milliardenschwere Schäden an. „Die Attacken sind zum Teil existenzbedrohend“, sagt der IT-Experte. Mit einem wahren Dauerfeuer versuchen virtuelle Gangster, in bestehende Netzwerkstrukturen einzudringen und sie zu korrumpieren.

Die Zahlen sind erschreckend: „Täglich werden 380 000 neue Schadprogrammvarianten losgeschickt“, sagt Paulus. Bislang konnte auf die Angriffe nur reagiert werden, jetzt ist man dabei, frühzeitig die Cyber-Angreifer zu entwaffnen. Gemeinsam mit dem österreichischen Hersteller Blue Shield Security GmbH haben die Schwandorfer eine IT-Lösung auf den Markt gebracht, die die Internetsicherheit revolutionieren dürfte. Blue Shield Umbrella heißt dieses neue innovative Konzept, für das das Deutsche Systemhaus bereits mit dem IT-Innovationspreis 2017 der Initiative Mittelstand ausgezeichnet worden ist.

Den Rechner mit Schadsoftware zu infizieren, ist beängstigend einfach. Da genügt es, verseuchte E-Mail-Anhänge zu öffnen, präparierte Websites aufzurufen oder manipulierte Werbebanner anzuklicken. Die Programme nisten sich sofort, für den ahnungslosen Internet-Surfer unbemerkt, auf seinem Rechner ein. Die Folgen – sie sind verheerend. Als Ransomware bekannte Erpressungssoftware sperrt zum Beispiel Festplatten, die man gegen Zahlung eines Lösegelds wieder freikaufen kann, bei CEO Fraud wird, unter Verwendung falscher Identitäten, Firmen manipuliert Geld überwiesen und unter der Wucht von Botnet-Attacken brechen Websites zusammen. Die Hacker haben aber schon eine neues Ziel im Visier: Industrie 4.0 und das Internet der Dinge. Vernetzte Maschinen können manipuliert und so im schlimmsten Fall die Produktion zum Erliegen gebracht werden.

Christian Paulus, Geschäftsführer der Deutsche Systemhaus GmbH, (li.) und Alois Kobler, Geschäftsführer der Blue Shield Security GmbH, stellten Blue Shield Umbrella auf der IT-Security-Messe it-sa in Nürnberg dem Fachpublikum vor. Foto: Paulus

„Die Cyber-Attacken werden immer komplexer“, weiß Paulus. Trotz Firewall, Sandboxsystemen und Endpoint Protection, mit denen sich die Unternehmen bislang abschirmen, gelingt es den Kriminellen relativ mühelos, immer wieder diese Schutzmauer zu durchbrechen. Paulus wundert das nicht. „Die Mehrheit der IT-Sicherheitslösungen nutzt heuristische Methoden und Signaturen.“ Die Antiviren-Software zum Beispiel basiert auf der Technologie der 80er-Jahre. Und auch sogenannte Sandboxing-Lösungen haben fast schon ausgedient. Die kriminellen Tüftler haben es tatsächlich geschafft, dass ihre Schadprogramme diese drohende Sandkasten-Isolierung erkennen und ihr entkommen. „Ist aber die Malware erst einmal im Netzwerk, sind wirksame Gegenmaßnahmen häufig schon zu spät“, erläutert der Sicherheitsexperte.

Genau hier setzt die cloudbasierte Blue-Shield-Umbrella-Lösung an. Die Prüfung findet außerhalb des eigenen Netzwerks statt. Potenzielle Schadsoftware gelangt nicht mehr ins LAN. Und so funktioniert es: Um einen Angriff zu verhindern, muss der Name des kompromittierenden Systems bekannt sein und gesperrt werden. Aber nicht mehr, wie bislang üblich, bei den sogenannten Root-DNS-Servern, sondern nun wird bei den Intelligence DNS Centern um die Namensauflösung angefragt. Diese wiederum kommunizieren mit dem European Threat Intelligence Defence Center, bei dem die Datenbankserver stehen, die mit den Ergebnissen aus mathematischen Bedrohungs-Wahrscheinlichkeitsberechnungen und Informationen der größten IT-Security-Hersteller gefüttert werden. Dort wird in Echtzeit der angefragte Name bewertet. Ist der gesperrt, wird der anfragende Server informiert und die Klienten bekommen eine Mitteilung über den Verbindungsstopp. Verhindert wird damit auch automatisch das Nachladen von Schadcodes, zudem werden vorhandene Botnetze und Trojaner abgeschaltet.

Sechs Jahre lang wurde an der Entwicklung des Blue Shield Umbrella gearbeitet. Eine Sicherheitslösung, an der sich, nach Ansicht von Paulus, die Hacker für die nächsten Jahre gründlich die Zähne ausbeißen werden: „Aufgrund des Einsatzes dynamischer mathematischer Algorithmen, die kontinuierlich weitergeschrieben werden, werden wir immer die Nase vorne haben.“ Aber nicht nur der Sicherheitsaspekt spricht für das innovative Konzept. Für den Blue Shield Umbrella, der in alle gängigen Betriebssysteme implementiert werden kann, muss weder eine Software installiert werden, noch müssen zusätzliche Rechnerleistung oder Arbeitsspeicher abgezweigt werden. Updates gibt es nicht und auch der administrative Aufwand ist gleich null.