Suchtreffer 1 von 3

Anlagen:

PDF-Artikel

PDFWW20110328028.pdf

WirtschaftsWoche NR. 013 VOM 28.03.2011 SEITE 029

Verschlungene Wege

Cyberangriff | Hacker-Attacken könnten die nächste Katastrophe auslösen. Versicherungen richten ein privates Abwehrzentrum ein.

Axel Wehling verstößt gegen alle Regeln, die Lehrbücher für eine erfolgreiche Unternehmensgründung empfehlen. Der Firmenname ist so unaussprechlich, dass sich ihn niemand merken kann. Das Unternehmen verfolgt ausdrücklich nicht den Zweck, Gewinne zu erwirtschaften. Selbst die fünf Festangestellten machen im Hauptberuf eigentlich etwas ganz anderes, stehen aber für den Notfall immer bereit.

Wehling ist Geschäftsführer der LKRZV GmbH, des Krisenreaktionszentrums für IT-Sicherheit der deutschen Versicherungswirtschaft. Hinter dem sperrigen Namen versteckt sich die erste private Cyberpolizei, die in Deutschland ihren Dienst im Internet aufgenommen hat. Rund um die Uhr, 365 Tage im Jahr patrouillieren fünf im LKRZV zusammengezogene IT-Experten in den Kommunikationsnetzen der Versicherer. Sie suchen nach Anomalien im Web, wehren Cyber-attacken ab, ziehen Lehren aus den sich ständig wandelnden Angriffsformen und leiten - was das Wichtigste im Ernstfall ist - ihre Erkenntnisse direkt an alle Mitglieder des Gesamtverbandes der Deutschen Versicherungswirtschaft (GDV) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) weiter.

Ein zentraler Ansprechpartner für Cyberkrisen - davon träumt auch die Bundesregierung schon länger. Regierungsvertreter preisen den "Modellcharakter" dieser in aller Stille aufgebauten Einrichtung. Dabei ist die Idee gar nicht neu: Schon vor rund vier Jahren hatten 30 Industrievertreter mit dem Bundesinnenministerium einen "Nationalen Plan zum Schutz kritischer Infrastrukturen" verabschiedet und sich darin verpflichtet, für jede Branche solch ein Abwehrzentrum einzurichten. Doch bei dem Plan ist es geblieben. So lebenswichtige Branchen wie Energie, Wasser oder Banken schludern beim Kampf gegen Hacker und Cyberkrieger und verzichten bis heute auf ein eigenes Krisenreaktionszentrum.

Zwei Wochen nach der Atomkastastrophe in Japan wächst der Druck auf die Betreiber kritischer Infrastrukturen, diese Sicherheitslücke zu schließen. Erstmals sind mit dem Erdbeben, dem anschließenden Tsunami und den dadurch außer Kontrolle geratenen Atommeilern drei statistisch unwahrscheinliche Ereignisse gleichzeitig eingetreten: Jetzt droht der Super-GAU. Überall in der Welt müssen bislang undenkbare Risiken neu bewertet werden.

Auch in Deutschland könnte ein Stromausfall eine Kettenreaktion ähnlich katastrophale Folgen auslösen. Cyberkrieger könnten etwa das Chaos nach einer Naturkastastrophe nutzen und die IT-Systeme lebenswichtiger Infrastrukturen lahmlegen und zum Absturz bringen. Die Bundesregierung will darum von der Industrie wissen, ob es Hintertüren in den IT-Systemen gibt. Auch die Atomkraftwerksbetreiber sollen nachweisen, dass die Computersysteme der Anlagen vor Cyberangriffen sicher sind, fordert Bundeskanzlerin Angela Merkel.

Der erste Schritt ist die Gründung des neuen Cyberabwehrzentrums - am 1. April nimmt es seine Arbeit in der Bonner BSI-Zentrale auf. Oberstes Ziel ist, das bisher recht unkoordinierte Vorgehen diverser staatlicher Stellen zu "optimieren". Verschlungene Wege soll es ncht geben. Ob das gelingt, ist aber fraglich.

Brüderle formt Task Force Denn Bundeswirtschaftsminister Rainer Brüderle will schon in der nächsten Woche die Mitglieder einer eigenen Task Force vorstellen, die sich speziell um die IT-Sicherheit kleiner und mittlerer Unternehmen kümmert. Gleichzeitig drängt das Innenministerium die Industrie zum Aufbau weiterer privater Cyberabwehrzentren, damit im Ernstfall die Betreiber kritischer Infrastrukturen ohne Zeitverzug Gegenmaßnahmen einleiten können.

Die Deutsche Telekom wittert darin ein neues Geschäftsfeld und fordert ein übergreifendes Lagezentrum der gesamten Industrie. "Beim Aufbau und Betrieb können wir unser Know-how einbringen", hat Telekom-Vorstand Reinhard Clemens, zugleich Chef der IT-Sparte T-Systems, großzügig angeboten. Anfangen sollte er am besten in der eigenen Branche. Die konkurrierenden Interessenverbände konnten sich noch nicht auf ein zentrales Abwehrzentrum verständigen.

Berke, Jürgen

28. März 2011