

„Kein Platz für Beliebigkeit“



Lennart Oly, Geschäftsführer der ENX Association

Die Automobilindustrie befindet sich im Fokus der Wirtschaftsspionage. Dies gilt gerade in einer wirtschaftlichen Lage, in der über den Fortbestand von Unternehmen entschieden wird. Internetgebundene Angriffe auf Netzwerke und Systeme sind dabei laut Verfassungsschutzbericht die aktuell gefährlichste Bedrohung.

Viele Unternehmen schützen zwar ihre eigene Infrastruktur, stoßen aber an Grenzen, sobald Verschlüsselungs- und Authentifizierungslösungen unternehmensübergreifend eingesetzt und als vertrauenswürdig anerkannt werden müssen. Das Ergebnis ist allzu oft Be-

liebigkeit. Es wird ein Blumenstrauß an Einzellösungen geschaffen, die jeweils die Wahrnehmungsschwelle des Managements unterschreiten. Sie gelten häufig als „nicht strategisch“, verstecken sich in vielen kleinen Einzelpositionen im IT-Budget und entziehen sich TCO-Betrachtungen ebenso wie einer ernsthaften Sicherheitsanalyse.

Insellösungen, die per se kostengünstig sein sollen, führen bei Partnern, die eine Vielzahl von Kunden bedienen, zu hohem Aufwand. Spätestens wenn beide Seiten jeweils eigene Mechanismen durchsetzen wollen, endet dies häufig in der Sackgasse. Das zeigt sich am Beispiel der E-Mail-Sicherheit und tausenden

der unverschlüsselter Datenleitungen in Entwicklung und Logistik. So können die CIOs keine sinnvolle Governance über ihre unternehmensübergreifende IT-Sicherheit ausüben. Die Antwort ist, existierende Standards und Lösungen systematisch zu stärken, Individualanforderungen kritisch zu hinterfragen und bestehende unternehmensübergreifende Lösungen mit zu gestalten und sich aktiv einzubringen.

Es gilt, das geistige Eigentum einer Industrie zu schützen, die gerade die vielleicht wichtigsten Forschungs- und Entwicklungsschritte der letzten Jahrzehnte unternimmt. Für irgendeine Form von Beliebigkeit ist hier kein Platz.

ALARM IM WEB

DIE UNIVERSITÄT BREMEN FORSCHT AN EINEM SPEZIELLEN FRÜHWARNSYSTEM FÜR IT-SYSTEME MIT WEBANBINDUNG.

Die Angriffe auf IT-Systeme werden immer professioneller. Datenspiegung hat längst die Dimension von organisierter Kriminalität angenommen. In Reaktion darauf will das Technologie-Zentrum Informatik und Informationstechnik (TZI) an der Universität Bremen – in dem Projekt „FIDeS“ (Frühwarn- und Intrusion Detection System) – zusammen mit Partnern eine Art Alarmanlage entwickeln. „Wir betreiben hier, ausgehend von den konkreten Anforderungen beteiligter Unternehmen wie T-Systems oder dem Zulieferer ZF Friedrichshafen, anwendungsorientierte Forschung. Ziel

ist ein Prototyp, der später zu einem Produkt ausgebaut werden kann“, erklärt der technische Projektleiter Karsten Sohr vom TZI. Das Institut für Internet-Sicherheit der Fachhochschule Gelsenkirchen bringt als wissenschaftlicher Hochschulpartner ein bewährtes Internet-Analysesystem ein, das die Daten verschiedener Internetprotokolle streng anonymisiert erfasst und auswertet.

Bei großen Unternehmen können das Millionen von Transaktionen in der Minute sein. „Die Herausforderung des Projektes ist es, diese verschiedenen Pro-

tokollquellen in der Analyse zusammenzuführen und Angriffe von systeminternen Abweichungen zu unterscheiden“, berichtet Norbert Pohlmann vom Institut für Internet-Sicherheit.

Untersucht werden dabei Protokolle wie HTTP oder SMTP und Technologien wie Voice over IP oder die serviceorientierte Architektur (SOA). Drei Jahre haben die Bremer Wissenschaftler Zeit, dieses Problem zu lösen. Gelingt das, hätte die IT-Security in den Unternehmen ein neues Werkzeug gegen Hacker in der Hand.

Autor: Frank Dresen