IFIT - Freies Institut für IT-Sicherheit e.V.

Pressemitteilung „Freies Instituts für IT-Sicherheit e.V.“ (IFIT)

Wie sicher sind die Daten der NSA oder was bedeutet der aktuelle Abhörskandal für mittelständische Unternehmen in der Region Weser-Ems?

Bremen, 10. November 2013. Durch das Bekanntwerden der Abhör- und Überwachungstätigkeiten durch die Geheimdienste in einer nie geahnten Dimension sind viele Menschen verunsichert. Doch während sich alles auf Edward Snowden konzentriert, wird weltweit munter weiterspioniert. Die Frage nach angemessenen Konsequenzen des nunmehr seit Monaten diskutierten Abhörskandals wird möglicherweise nie beantwortet werden können. Zu komplex sind die internationalen politischen Verflechtungen. Wer hat wann was gewusst, mitgewirkt oder profitiert? Politische Kommentare sind an Unbedarftheit nicht zu überbieten. Dass Geheimdienste weltweit tätig sind und versuchen, jede nur erdenkliche Informationsquelle zu nutzen, ist aber nichts Neues für jeden, der sich mit dem Sinn von Nachrichtendiensten auseinandersetzt.

Es ist auch hinlänglich bekannt, dass wie selbstverständlich Unternehmen systematisch und nahezu flächendeckend von Geheimdiensten und, was eher zu erwarten ist, von der internationalen Wirtschaftskonkurrenz angegriffen werden, um Know-how und Unternehmensstrategien anzuzapfen. Anders als ein gewöhnlicher Hacker, der Schaden verursachen möchte, haben solche Organisationen kein Interesse daran aufzufallen. So gelingt es, über Monate, ja Jahre hinweg, Informationen zu erlangen und für sich zu verwenden. Leichtsinn und unzureichendes Bewusstsein über die eigene Gefährdungssituation machen es den Angreifern leicht. Wenn es sogar 14-jährigen Skriptkiddies gelingt, in vorgeblich gut gesicherte Netzwerke einzudringen, was können dann erst hervorragend ausgebildete Computerfachleute, möglicherweise unterstützt durch ein Land und ausgestattet mit Hightech, anrichten?

Die Methoden reichen vom Systemeinbruch eines Wirtschaftsspions, dem klassischen "Hacken" eines Netzwerkes, dem Einschleusen von Personal, bis hin zur Erpressung oder einem Einbruch. Es hat schon Fälle gegeben, da wurde bei einem Einbruch nichts entwendet, sondern heimlich etwas hinzugefügt, nämlich eine Abhöranlage oder ein Computerprogramm.

Nach Meinung von Bernd Frenz, Mitglied im Freien Institut für IT-Sicherheit e.V. (IFIT) und Inhaber von IFIS-FR, Ingenieurbüro für Informationssicherheit, hat der Fall Snowden dabei auch eine andere Dimension, die in der bisherigen Diskussion bisher nicht im Fokus steht: Wie konnte ein externer Mitarbeiter eines Geheimdienstes an diese Menge von geheimen Daten und Informationen gelangen? Das, was dort im großen Stil gelang, kann überall passieren, und es passiert tagtäglich in unzähligen Unternehmen. Natürlich kann man sich als einfacher Bürger freuen, wenn Steuerdaten angekauft und die Sünder zur Rechenschaft gezogen werden. Aber auch hier muss man sich fragen, warum es scheinbar so einfach ist, derart brisante Daten aus einer Bank mitzunehmen? Wenn es sogar bei einem Geheimdienst oder einer Bank funktioniert, wäre es wohl ungleich einfacher, das Wissen eines mittelständigen Unternehmens zu erlangen.

In Bremen und dem Umland sind sehr viele Unternehmen angesiedelt, die über sehr großes Know-how in ihrem Marktsegment verfügen oder sogar Innovationsführer sind. Vielen ist das möglicherweise gar nicht ausreichend bewusst. Die internationale Konkurrenz hat ein sehr großes Interesse, dieses Wissen zu erlangen. Beispielsweise unterhalten Logistikunternehmen hochkomplexe Steuerungssysteme für die Warenströme. Nicht auszudenken was passiert, wenn jemand die Daten durcheinanderbringt. Gerade mittelständische Unternehmen sind besonders gefährdet, weil Sie oft aufgrund ihrer Größe keine eigenen Sicherheitsfachleute beschäftigen. Auch glauben viele, dass sie zu uninteressant seien, um als Zielobjekt für Wirtschaftsspionage zu dienen.

Unter wirtschaftlichen Gesichtspunkten ist ein 100%iger Schutz der gesamten Infrastruktur und aller Anwendungen im betrieblichen Alltag utopisch. Was sind aber praktikable Antworten für den Mittelstand in der Region zu den aufgekommenen Sicherheitsfragen?

Das IFIT als Kompetenz-Netzwerk von Sicherheitsexperten in der Region liefert dazu Antworten. Der erste Schritt ist die Bewusstseinsbildung über die eigene Verwundbarkeit, verbunden mit dem Willen, ein angemessenes Sicherheitsmanagement zu implementieren. Der klassische Ansatz mit einem „Stück Firewall“ und „etwas Virenschutz“ hilft nur sehr begrenzt. Stattdessen ist die Kenntnis der unternehmenswichtigen Ressourcen und Informationen von elementarer Bedeutung. Diese „Kronjuwelen“ lassen sich dann nach Analyse bestehender Gefährdungen und Risiken angemessen und effizient schützen.

Freies Institut für IT-Sicherheit e.V. (IFIT)

Das IFIT wurde von Experten aus der Praxis initiiert und ist im Jahr 2007 aus dem *„Bremer Security Forum“* hervorgegangen. Zweck des Vereins ist es, ein Kompetenz-Netzwerk zu bilden, um Unternehmen und Institutionen der gewerblichen Wirtschaft, sowie öffentliche Einrichtungen vornehmlich in den Bundesländern Bremen und Niedersachsen mit dem Schwerpunkt Weser-Ems

- in Fragen der IT-Sicherheit bzw. Informationssicherheit zu informieren,
- den Informationsaustausch zwischen den Mitgliedern zu fördern
- und die “gelebte Sicherheit“ in den Unternehmungen zu verbessern.

Seit August 2013 ist das IFIT offizieller Multiplikator der Allianz für Cybersicherheit, einer Initiative des Bundesamts für Sicherheit in der Informationstechnik (BSI), die 2012 in Zusammenarbeit mit dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) gegründet wurde.

Alle Infos finden Sie unter http://www.ifitev.de.

Verantwortlich und Pressekontakt: Stefan Menge, Vorstandsvorsitzender, Freies Institut für IT-Sicherheit e.V. (IFIT), Bremen, Telefon 0171 – 55 80 135, menge@ifitev.de