Pressemitteilung
Sankt Augustin, 08.02.2013

Melden allein macht nicht sicher

Ablehnung der Meldepflicht von ‚Cyber-Attacken'

1. Mit der bereits 2012 vom **Innenminister Friedrichs** für die Bundesrepublik und jetzt von der EU-Telekomkommissarin **Neelie Kroes** für die gesamte EU erneut vorgeschlagenen Richtlinie zur sog. Netz- und Informationssicherheit zur **Meldepflicht von Angriffen und Datenpannen** an den Staat kann das Internet nicht vor kriminellen und terroristischen Angriffen geschützt werden: Melden allein schützt nicht!
2. Die wenigen Unternehmen und Behörden, die heute immer noch nicht hinreichend abgesichert sein sollten, erkennen Angriffe sowieso nicht und haben dann auch **gar nichts zu melden**!
3. Das Ziel einer besseren Abwehr von Internetangriffen ist durch das Zählen der Datenpannen gar nicht erreichbar. Das Meldeverfahren von Angriffen geht also in die **falsche Richtung**: Es täuscht Sicherheit nur vor.
4. Große Unternehmen werden 100.000-mal pro Tag angegriffen. Bei ca. 40.000 relevanten Unternehmen in der EU ergeben sich bei durchschnittlich nur 50 Angriffen pro Tag **2 Mio. Datensätze**, die ja auch täglich sehr zeitnah abschließend und vollständig europaweit ausgewertet werden müssen.
5. Im Vorschlag überwiegt also der Aufbau einer weiteren Bürokratie und / Verwaltungsstruktur zur Sammlung von Daten: **Hoher Verwaltungsaufwand** ohne jeglichen erkennbaren Nutzen.
6. **Meldepflichtig** sollen vor allem Unternehmen der Kritischen Infrastrukturen sein – also lebenswichtige Unternehmen - sein wie Banken, Energieversorger, Verkehrsunternehmen und Krankenhäuser, öffentliche Verwaltungen sowie Internetanbieter wie auch App Stores, Suchmaschinen oder soziale Netzwerke. Anbieter von Internetdiensten unterliegen allerdings bereits heute schon einer Meldepflicht!
7. Angriff auf das Internet und die IT von Unternehmen sind nur dann erfolgreich, wenn Software **Sicherheitslücken** enthält. Um das Übel der Angriffe auf das Internet in den Griff zu bekommen, müssen die von den Angriffen ausgenutzten Sicherheitslücken identifiziert und dann auch behoben werden: Das Übel muss an der Wurzel gepackt werden!
8. Sicherheitslücken werden allerdings häufig von den Software-Herstellern nur zur Kenntnis genommen und nicht sorgfältig **zeitnah behoben**; vielfach werden die Kunden auch nicht über diese Sicherheitslücken informiert, so dass sie Angriffen schutzlos ausgeliefert sind.
9. Die Gesellschaft für Informatik hat bereits vor 3 Jahren (2009) gefordert, Sicherheitslücken zu veröffentlichen, damit sich Unternehmen schützen können: „Die Bundesregierung muss alle ihr bekannt gewordene Sicherheitslücken und diese ausnutzende Schadprogramme unverzüglich veröffentlichen".

Kontakt:
Prof. Dr. Hartmut Pohl
Tel.: 02241 – 255 43 – 0
Fax: 02241 – 255 43 – 29
Hartmut.Pohl@softScheck.com

softScheck GmbH
Bonner Straße 108
53757 Sankt Augustin
www.softScheck.com