Alarm bei Cyber-Angriffen

Darmstadt (HE). **Die jüngste Cyber-Attacke mit der Schadsoftware „WannaCry“ hat es weltweit deutlich gezeigt: Die IT in Unternehmen und vor allem in Kritischen Infrastrukturen (KRITIS) ist angreifbar. Der aktuelle Fall hält uns deutlich vor Augen, wie schnell die KRITIS weltweit ausfallen könnten. Dieses Mal hat es z. B. Krankenhäuser, Banken, Telekommunikationsgroßkonzerne und die Deutsche Bahn getroffen.**

Die Cyber-Attacke zeigte, wie hilflos und handlungsunfähig beispielsweise das Personal in den Krankenhäusern wird, wenn die IT ausfällt. Die Mitarbeiter konnten nicht mehr auf Patientendaten zugreifen und z. B. Raum- bzw. Terminplanungen aufrufen. Viele Patienten wurden nach Hause geschickt oder in andere, nicht betroffene Kliniken verlegt.

Noch schlimmer hätte es kommen können, wenn der Virus den lokalen Netzversorger angegriffen und die Stromversorgung für die Kliniken lahmgelegt hätte.

Doch egal, wie schlimm es die IT in den Klinken und in anderen Unternehmen und Organisationen getroffen hätte, eines hätte problemlos funktioniert: Die Alarmierung von Menschen.

Unsere Alarmsoftware GroupAlarm ist von der lokalen IT des Kunden abgekoppelt und läuft georedundant auf eigenen Servern von in Deutschland ansässigen Rechenzentren. Die Nutzer in den Kliniken rufen die Anwendung über den Browser des PCs – was im Fall von „WannaCry“ nicht funktionierte – oder per Tablett oder Smartphone auf. So können beispielsweise Techniker, Ärzte, Pflegepersonal über einen Ausfall schnell benachrichtigt werden sowie bei einem Totalausfall der IT gemäß den Notfallplänen koordiniert, alarmiert und benachrichtigt werden.

Text, Foto: Hanno Heeskens cubos Internet GmbH

THEMENINFO

Generelle Anmerkung des Niedersächsischen Ministeriums für Inneres und Sport zur Cybersicherheit

In einer Landtagsanfrage zum Thema Cybersicherheit schickte die Landesregiung folgende Anmerlkung zur Klärung der Zuständigkeiten vorweg:

Der Begriff „Computer Network Operations (CNO)“ ist sprachlich der operativen Cyberverteidigung zuzurechnen.
Wikipedia 1 beschreibt CNO wie folgt: „Computer Network Operations (CNO; deutsch Computer-Netzwerk-Operationen) ist ein militärischer Begriff, der mehrere Unterbegriffe umfasst.“ Konzepte hierfür werden in den Medien auch unter Stichwort „Hack-Back“ diskutiert und gehen von der Überlegung aus, Maßnahmen zur Beeinträchtigung von fremden Informations- und Kommunikationssystemen sowie der darin verarbeiteten Informationen durchzuführen, um fremde Cyberangriffe nachhaltig zu stören. Grundsätzlich geht es dabei um offensive Cyberstrategien, bei denen man bei der Bewertung zwischen Maßnahmen der äußeren Sicherheit (Bundeswehr im Zuständigkeitsbereich des Bundesverteidigungsministeriums) und denen der inneren Sicherheit (Strafverfolgung, Gefahrenabwehr) unterscheiden muss.

In Deutschland liegt die zentrale Zuständigkeit für Cybersicherheit auf Bundesebene beim Bundesministerium des Inneren, im Bereich der Länder bei den Landesinnenministerien. Da Cyberangriffe die Motivation der Angreifer (krimineller, politischer oder militärischer Hintergrund) zumeist nicht sofort erkennen lassen, kann neben der Zuständigkeit der Innenressorts auch eine Zuständigkeit des Bundesverteidigungsministeriums gegeben sein.

Nds. Innenministerium des Innern und Sport