Medien-Information

11. November 2019

Nach Attacken von Cyber-Erpressern auf kleine und mittelständische Betriebe: Land und Wirtschaft richten "Servicepoint Cybersecurity" als Anlaufstelle ein

KIEL. Die Attacke kam ebenso unerwartet wie leise aus dem Internet: Ein Hacker-Angriff legte im September die Produktion des Schwarzenbeker Tablettenmaschinen-Herstellers "Fette Compacting" lahm. Knapp vier Wochen später konnte das Unternehmen zwar Entwarnung geben, doch der Schaden durch den Produktionsausfall ist erheblich. Wenige Monate zuvor hatte ein Unternehmen aus dem Kreis Segeberg 800.000 Euro Lösegeld per Bitcoin an ausländische Erpresser gezahlt, um wieder an seine Daten zu gelangen.

Zwei von vielen Beispielen, die für Wirtschaftsminister Dr. Bernd Buchholz zeigen: "Cyber-Attacken sind kein Science-Fiction-Stoff, sie sind bittere Realität und längst auch im Alltag von kleinen und mittelständischen Unternehmen in unserem Land angekommen." Während die Hintergründe der bisherigen Fälle noch von Polizei-Experten untersucht und darum keine Einzelheiten bekannt gegeben werden, gehen Land und Wirtschaft jetzt in die Offensive: Zusammen mit Lars Müller, dem Vorsitzenden des Vereins Digitale Wirtschaft Schleswig-Holstein (DiWiSH), dessen Fachgruppenleiter für IT-Sicherheit, Andreas Sellin, und Kiels IHK-Hauptgeschäftsführer Jörg Orlemann gab der Minister heute den Startschuss für den "Servicepoint Cybersecurity".

Dabei handelt es sich um eine unabhängige Stelle bei der vom Land zu zwei Dritteln geförderten DiWiSH zur Vermittlung von Fachfirmen, die IT-Bedrohungen bekämpfen oder präventiv aktiv werden. Hintergrund des Angebots ist eine im August zwischen dem Land, der DiWiSH, der IHK Schleswig-Holstein und der "Allianz für Sicherheit in der Wirtschaft Norddeutschland e. V." (ASWN) besiegelten Sicherheitspartnerschaft. Wie Buchholz, Müller, Orlemann und Sellin erläuterten, soll ab Februar unter anderem über Informationsveranstaltungen dafür gesorgt werden, dass insbesondere kleine Betriebe in ihre IT-Sicherheit investieren und nicht erst aktiv werden, wenn ein Angriff erfolgreich war.

"Der Servicepoint ist dabei nur als neutraler Vermittler tätig", so Buchholz. Es konnten bereits neun Partnerunternehmen der Initiative gefunden werden. Dabei handelt es sich um AMC Business IT GmbH (Kiel); ascendit GmbH (Bordesholm); Consist Software Solutions GmbH (Kiel); fat IT solutions GmbH (Kiel); Hanko GmbH (Kiel); intersoft consulting services AG (Hamburg); L und M Business IT GmbH (Kiel); MELTING MIND (Lübeck); NetUSE AG (Kiel).

"Der Schutz von Kundendaten, als auch von Betriebs- und Geschäftsgeheimnissen muss in vielen Firmen einen höheren Stellenwert erlangen als es bislang vielfach der Fall ist", mahnt Buchholz. Auch Kiels IHK-Chef Orlemann betont, dass die Unternehmen in Schleswig-Holstein künftig noch besser vor On- und Offline-Kriminalität geschützt werden müssen: "Unsere Partnerschaft erhöht die Sicherheit unserer Unternehmen präventiv, schafft Angebote zu sicherheitsrelevanten Themen und warnt vor aktuellen Bedrohungen. Beim Servicepoint Cybersecurity kann sich die Wirtschaft Hilfe holen – anonym, professionell, unkompliziert und das nicht erst, wenn es bereits schiefgegangen ist."

Und DiWiSH-Chef Lars Müller appelliert: "Von Cyberattacken betroffene Unternehmen sollten über ihren Schatten springen und besonnen handeln. Denn jede Organisation kann Opfer werden. Es gilt, professionelle Hilfe in Anspruch zu nehmen - entweder von Sicherheitsbehörden oder bei DiWiSH-Mitgliedern, die auf IT-Sicherheit spezialisiert sind. Unser Servicepoint sorgt für eine neutrale Vermittlung zu passenden Experten. Zusätzlich ist es im betrieblichen Alltag wichtig, sich mit präventiven Maßnahmen zu befassen. Auch hier können wir helfend unterstützen."

Nach den Worten des IT-Sicherheitsexperten Andreas Sellin ist jedes Unternehmen gut beraten, regelmäßige Backups seiner Daten anzulegen und diese auch zu überprüfen. "Backups müssen von der normalen IT getrennt sein, damit keine Verschlüsselung der Daten erfolgen kann. Darüber hinaus ist ein gutes Notfallmanagement wichtig, um im Fall der Fälle geordnet alle im Notfallhandbuch aufgeführten Maßnahmen abzuarbeiten. Und es ist sinnvoll, Notfallszenarien immer mal wieder durchzuspielen", so Sellin. Ebenso wichtig seien regelmäßige Mitarbeiter-Schulungen und Informationen über aktuelle Bedrohungen.

Zu erreichen ist der Servicepoint Cybersecurity wie folgt:
0431 6 66 66-333
kontakt@servicepoint-cybersecurity.de
www.servicepoint-cybersecurity.de

Verantwortlich für diesen Pressetext: Harald Haase | Ministerium für Wirtschaft, Verkehr, Arbeit, Technologie und Tourismus | Düsternbrooker Weg 94, 24105 Kiel | Telefon 0431 988-4419 | Telefax 0431 988-4705 | E-Mail: pressestelle@wimi.landsh.de | Medien-Informationen der Landesregierung im Internet: www.schleswig-holstein.de | www.schleswig-holstein.de/wirtschaftsministerium