Husumer Nachrichten

CYBER-ATTACKE AUF BEHÖRDE

Auch Angriffe auf Nordfriesland: Ist der Kreis gut gegen Hacker gewappnet?

Hacker-Angriffe häufen sich: In Sachsen-Anhalt wurde ein gesamter Landkreis lahmgelegt. Wie ist die Lage in Nordfriesland?

Im Landkreis Anhalt-Bitterfeld in Sachen-Anhalt funktioniert derzeit nur noch die Telefonanlage. Das gesamte Betriebssystem wurde durch einen Hacker-Angriff lahmgelegt, zudem wird die Behörde erpresst. Wie sieht es in NF aus?

von **Jonna Marlin Lausen und Birger Bahlo**
14. Juli 2021, 15:47 Uhr

NORDFRIESLAND | Ausnahmezustand im Landkreis Anhalt-Bitterfeld: Durch eine Windows-Sicherheitslücke verschafften sich Hacker Zugriff auf das Betriebssystem der Behörde und verschlüsselten alle Daten. Seitdem stehen alle Computer still. Keine Anfragen, keine Kindergeldanträge, keine Auskunft vom Gesundheitsamt, nur noch die Telefonanlage funktioniert. Mittlerweile bestätigte das Landeskriminalamt Sachsen Anhalt, dass die Hacker ein Lösegeld fordern, um die Daten wieder freizugeben.

Weiterlesen: Hacker-Angriff über IT-Dienstleister trifft viele Firmen

Stadt Husum gibt keine Auskunft

Ein Worstcase-Szenario, das – so werden sich wohl viele Landräte in Deutschland nun fragen – auch jeden anderen Landkreis treffen könnte, oder? Shz.de hat beim Kreis Nordfriesland und bei der Stadt Husum nachgefragt, wie es um die Sicherheit ihrer IT-Systeme bestellt ist.

Weiterlesen: Mürwiker und Lebenshilfe kämpfen sich zurück ins Leben

Hauptamtsleiterin Ira Rössel erklärt in knappen Worten, nichts sagen zu wollen: „Die Stadt Husum gibt keinerlei Auskunft zum Thema IT-Sicherheit im Rathaus. Ich bitte entsprechend um Verständnis dafür, dass ich keine sicherheitsrelevanten Informationen herausgeben kann."

Kreis registriert Angriffs-Versuche

Ähnlich lautet die Antwort vom Kreis. Dieser habe seinen eigenen IT-Betrieb eingestellt und die Aufgabe dem IT-Zweckverband Schleswig-Holstein (kommunit) übertragen. Zwar seien dem Kreis die Sicherheitsvorkehrungen des Verbandes bekannt, allerdings dürften darüber keine Angaben gemacht werden.

Doch ein kleines Statement lässt sich der Kreis dennoch entlocken: „Wir können sagen, dass diverse Sicherheitsebenen existieren, grundsätzlich alle Systeme mindestens zweifach oder dreifach ausgelegt sind und wir uns im IT-Zweckverband sehr gut aufgehoben fühlen", so der stellvertretende Pressesprecher Brian Zube.

Die Ausgaben für Sicherheitstechnik würden zunehmend steigen, denn der IT-Zweckverband registriere durchaus Angriffsversuche, „was uns ebenfalls Sorgen bereitet", so Zube. Sowohl technische Notfallpläne wie Ausweichrechenzentrum, Datensicherung, Standortvernetzung wie auch organisatorische Notfallkonzepte, Nutzung der Infrastruktur der anderen Verbandsmitglieder, unter anderem des Kreises Pinneberg, seien in den Betriebshandbüchern festgelegt und würden kontinuierlich weiterentwickelt, so Zube.

Der Mensch als Abwehrkraft

All solche technischen Vorkehrungen hält auch Thomas Holst von der Firma BT Nord in Husum für unerlässlich. Er gilt als Experte für IT-Sicherheit, betont aber einen anderen Punkt, den er für sehr viel bedeutungsvoller hält. Auch die stärksten technischen Kontrollen könnten nicht verhindern, dass Schadsoftware eben doch noch durchschlupft in die Maileingänge der Nutzer am PC. Bei den Nutzern sei anzusetzen. Daher richtet er den Blick auf die Schulung der Menschen. Sie hätten es im wahrsten Sinn des Wortes in der Hand, ob sie den Startknopf für Spionage, Viren oder Sperren ganzer Systeme drücken.

Ein Haufen Tricks

Die Tricks seien vielfältig und können hier nur in Stichworten wiedergegeben werden: „Honeypots" (Honigtöpfe), die gezielt Angreifer anlocken. Gefälschte Seiten, die denen der eigenen Bank oder des Energieversorgers gleichen und in die gutgläubig Benutzername und Passwort eingegeben würden. Mails, die so aussehen, als kämen sie vom Chef („CEO-fraud") und der weist Geldtransfers ins Ausland an. Ein solcher Angriff sei beispielsweise erfolgreich auf ein Geldinstitut in Nordfriesland verübt worden.

Auch interessant: IHK-Fachdialog Digitalisierung: Vom Serienbrief bis zum papierlosen Büro – wie digitale Prozesse Firmen herausfordern

Oder es gebe echt aussehende Seiten für Online-Bewerbungen – und schon sei der Weg in die Systeme der Behörden oder Unternehmen geöffnet. Der Ansatz von Holst ist somit: Schulen und schulen, um bei jedem Mausklick

Betrugsversuche erkennen zu können. Bleibt die Frage, ob genau dieser Weg neben aller Technik beim Kreis und der Stadt Husum im Blick ist.