Die Erpresser lauern im Internet auf

WIRTSCHAFT Cybercrime-Experte referierte vor Unternehmern in der CzW-„Wirtschaftsfrühstück"-Runde

Beim „Wirtschaftsfrühstück" des Clubs zu Wilhelmshaven konnte einem der Bissen im Hals stecken bleiben: Thema war die Internet-Kriminalität.

VON HARTMUT SIEFKEN

WILHELMSHAVEN – Immer neue Methoden bedrohen die Sicherheit im Internet. Wirtschaftsunternehmen sind insbesondere von Datenklau und Erpressung bedroht, berichtete gestern Sven Schwarz, Oberkommissar bei der Polizeiinspektion Wilhelmshaven-Friesland und Leiter der Projektgruppe Cybercrime, vor dem Club zu Wilhelmshaven. Clubpräsident Holger Ansmann begrüßte zum traditionellen „Wirtschaftsfrühstück" zahlreiche Betriebsinhaber und Geschäftsführer, leitende Angestellte und Vertreter aus Politik und Behörden, darunter auch die Bürgermeister Ursula Glaser (CDU) und Holger Barkowsky (SPD), im Hotel Kaiser.

Die Projektgruppe ist seit Anfang des Jahres installiert und mit vier Beamten besetzt. Ihre Aufgabe ist, verbrecherische Angriffe auf Computersysteme aufzuklären. „Wir befassen uns allerdings nicht mit Beleidigungen in sozialen Netzwerken oder gewöhnlichem Betrug, der mit Hilfe der normalen Kommunikationswege im Internet erfolgt; das zählt zur normalen Kriminalität", so Schwarz.

Seine Projektgruppe sei vielmehr dafür zuständig, wenn Rechner manipuliert würden, indem sie mit Schadsoftware infiziert würden. Unternehmen würden bevorzugt per E-Mail angegriffen, in deren Anhänge sich Trojaner verbergen. Die Anschreiben sähen durchaus plausibel und seriös aus. Es könnten Bewerbungen für eine Stelle im Unternehmen sein, angebliche Rechnungen etc.

Würden die angehängten Dateien geöffnet, dringe der Virus in den Rechner und in das gesamte Rechnernetz des Unternehmens ein und lege es lahm. Cerber sei solch ein gefürchteter Trojaner, der sämtliche Firmen-Daten verschlüsele. Zum Schluss steht die Erpressung: Entweder du zahlst, oder du siehst deine Daten nie wieder. Das kann für Unternehmen, vor allem für kleine und mittelständische, schnell existenzbedrohend sein.

Oft, so Schwarz, würden Firmeninhaber auf die Erpressung eingehen und sich erst bei der Polizei melden, wenn trotz Lösegeldzahlung die Erpressungen nicht aufhörten.

Die Täter zu ermitteln, sei schwierig. Sie agierten meistens aus dem Ausland heraus und arbeiteten unter elektronischen Deck-Adressen. Umso wichtiger sei es, in den Unternehmen ein Gefahrenbewusstsein zu entwickeln. Dazu zählt die Information der Mitarbeiter über die möglichen Gefahren. Im Zweifel sollte eine E-Mail von einem unbekannten Absender lieber nicht geöffnet werden, erst recht nicht, wenn keine weiteren Kontaktdaten zur Überprüfung der Seriosität angegeben werden.

Unternehmen, die das Internet als Vertriebsweg nutzen, seien häufig Ziel von DOS-Attacken (Denial of Service – Dienstverweigerung), führte Schwarz weiter aus. Der Angreifer nutze dabei eine Vielzahl gekaperter Rechner, deren Eigentümer davon gar nichts mitbekämen, um die Internetseite eines Unternehmens anzugreifen und durch die Masse der Zugriffe lahmzulegen. Dagegen helfe oft nur mehr Rechnerleistung, gegebenenfalls durch externe Anbieter.

Zum Schutz vor Datenverlust sei es unabdingbar, seine Daten so oft wie möglich auf externen Speichern zu sichern, riet der Cybercrime-Experte.

Oberkommissar Sven Schwarz (rechts), Leiter der Projektgruppe Cybercrime bei der Polizeiinspektion Wilhelmshaven, referierte vor dem Club zu Wilhelmshaven (CzW). Das Präsidium mit Hans-Günter Wieting, Holger Sothmann, Jochen Seeger und Präsident Holger Ansmann (von links) begrüßten dazu viele Gäste. WZ-FOTO: LÜBBE