Cyber Crime: Polizei und Staatsanwaltschaft oft machtlos

DDoS-Attacken, Schadsoftware und Datendiebstahl machen Shopbetreibern das Leben schwer. Polizei und Staatsanwaltschaft können diesen kriminellen Angriffen nach Ansicht von Experten oftmals nur tatenlos zusehen. Shopbetreibern bleibt nur der Weg zur Selbsthilfe.

Fast jeder fünfte Online-Händler (18,8 Prozent) wurde bereits einmal das Opfer eines Erpressungsversuches durch Kriminelle. Das Tatmittel hier: Das Internet. Dabei zählen DDos-Attacken (12 Prozent) und die Einschleusung von Schadsoftware (10 Prozent) zu den häufigsten Angriffsformen. Das sind die zentrale Aussagen der Studie "Informationssicherheit im E-Commerce 2014" von ibi research an der Universität Regensburg.

Stefan Rojacher, Sprecher von Kaspersky Lab, beziffert den Schaden, der zum Beispiel durch DDos-Attacken verursacht werden auf bis zu 360.000 Euro für die betroffenen Unternehmen:

> *"DDoS-Attacken zählen inzwischen zur Routine von Cyberkriminellen. Es hat sich sogar schon eine kleine ‚Industrie' gebildet, in der Botnetze verkauft werden. Der Schaden, der durch DDoS-Attacken verursacht wird, beträgt bei den Unternehmen im deutschen Mittelstand durchschnittlich 41.000 Euro, bei großen Unternehmen rund 360.000 Euro."*

Cyber Crime ist organisierte Kriminalität

Shopbetreiber sollten Erpressungsversuche nicht auf die leichte Schulter nehmen. Auf keinen Fall mit den Kriminellen auf Verhandlungen einlassen, warnt Studienautor Tobias Lehner von ibi research:

> *"In den meisten Fällen lassen die Erpresser ihren Drohungen auch sehr schnell Taten folgen. Daher raten wir Online-Händlern Erpressungsversuche auf jeden Fall zur Anzeige zu bringen."*

Doch was bringt eine Anzeige bei der Polizei? Nach Aussagen von IT-Sicherheitsexperten können Polizei und Staatsanwaltschaft in der Regel nur wenig tun, erklärt Lehner.

> *"Leider ist der Arm der Strafverfolgungsbehörden beim Thema Cyber Crime sehr kurz. Eine Ermittlung und Bestrafung der von professionellern Täterbanden gelingt nur in seltenen Fällen. Wenn die Polizei Erfolge aufweisen kann, dann sind es oftmals halbwüchsige Skript-Kiddies, die durch plumpe Hacker-Attacken aufgefallen sind."*

Die Hilflosigkeit der Polizei habe unter anderem damit zu tun, dass viele Cyber-Kriminelle in mafiöse Strukuturen eingebunden seien und zudem bestens ausgerüstet seien, weiß auch Rojacher.

> *"DDoS-Angriffe mit einhergehenden mafiaähnlichen Erpressungsszenarien und Cyberkriminalität machen nicht vor Landesgrenzen halt. Für die Verfolgung dieser Straftaten, die ohnehin schon sehr komplex ist und zahlreiche Ressourcen bei den Strafverfolgungsbehörden in Anspruch nimmt, ist dies eine zusätzliche Herausforderung. Aus diesem Grund arbeitet Kaspersky Lab eng mit supranationalen Polizeiorganisationen, wie Interpol oder Europol, in Sachen Cyber Crime zusammen."*

Online-Händler müssen sich also selber darum bemühen, ihre IT-Systeme abzusichern. Auch wenn

es einen vollständigen Schutz gegen Cyber-Crime-Angriffe nicht gebe, lasse sich die Gefahr Opfer einer Attacke zu werden, durch entsprechende Sicherheitskonzepte reduzieren, weiß Tobias Lehner. Dazu zählen sowohl technische Lösungen, als auch firmeninterne Schulungen der Mitarbeiter zum Thema Datensicherheit.