Achtung Holiday Season! Wie sich Online-Händler vor Cyber-Attacken schützen können

Es ist Holiday-Season! Vom Black Friday über Cyber Monday bis Weihnachten – am Ende des Jahres häufen sich die Shopping-Events und mit ihnen steigen die Umsätze im Online-Handel. Doch nicht nur im E-Commerce läuft das Geschäft jetzt auf Hochtouren, auch für Cyber-Kriminelle ist das Weihnachtsgeschäft lukrativ.

Besonders beliebt sind dabei sogenannte DDos-Angriffe auf Online-Shops. Am zurückliegenden Cyber Monday etwa registrierte das Link11 Security Operation Center (LSOC) mehr als doppelt so viele DDoS-Attacken auf E-Commerce-Anbieter als an den anderen Tagen im Jahr. Eine Cyber-Attacke kann schnell einen Schaden in Höhe von mehreren Hunderttausend Euro verursachen – sind Händler hier nicht abgesichert, steht im schlimmsten Fall die Existenz des Unternehmens auf dem Spiel.

DDoS-Attacken: Erhebliche Schäden durch Überlastung
DDoS steht für “Distributed Denial of Service” und ist eine spezielle Art des Angriffs von Cyber-Kriminellen, mit dem Ziel, die IT-Infrastruktur des Opfers zu überlasten und dadurch lahmzulegen. Die Folgen eines solchen IT-Ausfalls sind gerade in Hochzeiten wie in den Wochen vor Weihnachten für den Online-Handel fatal. So hat der Branchenverband Bitkom die Kosten verschiedenster Cyber-Angriffe, wie auch für den Fall einer Überlastungsattacke, berechnet: Selbst wenn ein Online-Händler nur knapp einen Tag offline ist, kann der Schaden, wie im Beispiel aufgeschlüsselt, bereits 185.000 Euro betragen. Eine Summe, die für die meisten Unternehmer eine finanzielle Katastrophe bedeutet. Hinzu kommt: Cyber-Kriminelle nutzen DDos-Angriffe, um von den betroffenen Unternehmen Lösegelder zu erpressen. Aus Sorge vor weiteren finanziellen Ausfällen lassen sich viele Unternehmer darauf ein – und zahlen am Ende doppelt.

Rechtzeitig schützen und an Folgen denken
Online-Händler sollten also gerade jetzt besonders aufmerksam sein, ihren Shop proaktiv schützen und sich Gedanken um eine mögliche Absicherung machen. Dabei lohnt es sich nicht nur an das Back- und Frontend zu denken, sondern auch die Folgen einer Cyber-Attacke, vor allem vor dem Hintergrund der DSGVO, im Blick haben. Der Abschluss einer Cyber-Versicherung kann im Ernstfall helfen. Kommt es zu einem Angriff und einer einhergehenden Unterbrechung des Geschäftsbetriebs, zahlt die Versicherung nicht nur eine vereinbarte Entschädigung für den Umsatzausfall, sondern bietet auch Notfall-Serviceleistungen an. Auf diesem Weg können auch die Auswirkungen von Datenschutzverletzungen der durch die neue DSGVO verschärfte Haftungssituation begrenzt werden. Von diesem Angebot profitieren gerade kleine und mittelständische Unternehmen, denen gewöhnlich entsprechende Ressourcen fehlen und die besonders häufig im Visier von Cyber-Kriminellen stehen.

Angebote vergleichen ist wichtig
Aktuell bieten auf dem deutschen Markt etwa 20 Versicherer Cyberversicherungen an. Der Vergleich der verschiedenen Produkte ist dabei nicht immer einfach, denn diese variieren mitunter stark. Zudem sind die Policen häufig in Modulen aufgebaut, sodass es umso wichtiger ist, die Angebote der Versicherer auf die individuelle Unternehmensstruktur hin zu prüfen. Einen zuverlässigen Überblick über die einzelnen Produkte bietet z.B. CyberDirekt an, hier finden Unternehmer das für sie passende Angebot.

Pressekontakt:

Miriam Graf
Telefon: 0159-02904502
E-Mail: miriam@monocerospr.com

Unternehmen
CyberDirekt
Internet: www.cyberdirekt.de