Achtung: Kriminelle ziehen Daten aus über 1.000 Online-Shops

Über 1.000 deutsche Online-Shops wurden von Kriminellen manipuliert, sodass Kundendaten und Zahlungsinformationen während des Bestellvorgangs an Kriminelle abfließen, berichtet das Bundesamt für Sicherheit in der Informationstechnik. Sichern Sie Ihren Shop, sonst drohen Bußgelder!

Das Bundesamt für Sicherheit in der Informationstechnik hat folgende Pressemitteilung herausgegeben:

Online-Skimming: 1.000 deutsche Online-Shops betroffen

Dem Bundesamt für Sicherheit in der Informationstechnik (BSI) liegen Informationen vor, nach denen aktuell mindestens 1.000 deutsche Online-Shops von Online-Skimming betroffen sind. Dabei nutzen Cyber-Kriminelle Sicherheitslücken in veralteten Versionen der Shopsoftware, um schädlichen Programmcode einzuschleusen. Dieser späht dann beim Bestellvorgang die Zahlungsinformationen der Kunden aus und übermittelt sie an die Täter. Betroffen sind Online-Shops, die auf der weit verbreiteten Software Magento basieren.

Der eingeschleuste Code und der damit verbundene Datenabfluss ist für Nutzer üblicherweise nicht erkennbar. Über den Umfang der über diese Angriffe bereits abgeflossenen Zahlungsdaten liegen dem BSI zur Zeit keine Erkenntnisse vor.

Basierend auf einer von einem Entwickler von Sicherheitstools für Magento durchgeführten Analyse wurden bereits im September 2016 weltweit knapp 6.000 von Online-Skimming betroffene Online-Shops identifiziert, darunter auch mehrere hundert Shops deutscher Betreiber. CERT-Bund benachrichtigte daraufhin die jeweils zuständigen Netzbetreiber in Deutschland zu betroffenen Online-Shops. Aktuellen Erkenntnissen zufolge wurde diese Infektion von vielen Betreibern bis heute nicht entfernt oder die Server wurden erneut kompromittiert. Die von den Angreifern ausgenutzten Sicherheitslücken in Magento wurden von den Shop-Betreibern trotz vorhandener Softwareupdates offenbar nicht geschlossen. Dies ermöglicht Cyber-Kriminellen, weiterhin Zahlungsdaten und andere bei Bestellungen eingegebene persönliche Daten von Kunden auszuspähen. Die Anzahl aktuell bekannter betroffener Online-Shops in Deutschland ist dadurch auf mindestens 1.000 angestiegen.

Das CERT-Bund des BSI hat heute erneut die jeweils zuständigen Netzbetreiber in Deutschland zu betroffenen Online-Shops in ihren Netzen informiert und bittet Provider, die Informationen an ihre Kunden (Shop-Betreiber) weiterzuleiten.

> *“Leider zeigt sich nach wie vor, dass viele Betreiber bei der Absicherung ihrer Online-Shops sehr nachlässig handeln. Eine Vielzahl von Shops läuft mit veralteten Software-Versionen, die mehrere bekannte Sicherheitslücken enthalten”, erklärt BSI-Präsident Arne Schönbohm. “Die Betreiber müssen ihrer Verantwortung für ihre Kunden gerecht werden und ihre Dienste zügig und konsequent absichern.”*

Nach § 13 Absatz 7 TMG sind Betreiber von Online-Shops verpflichtet, ihre Systeme nach dem Stand der Technik gegen Angriffe zu schützen. Eine grundlegende und wirksame Maßnahme hierzu ist das regelmäßige und rasche Einspielen von verfügbaren Sicherheitsupdates.

Das BSI weist an dieser Stelle darauf hin, dass die Verpflichtung zur Absicherung von Systemen nicht nur für Unternehmen, sondern auch für alle anderen geschäftsmäßigen Betreiber von Websites gilt. Darunter fallen zum Beispiel auch Websites von Privatpersonen oder Vereinen, wenn mit deren Betrieb dauerhaft Einnahmen generiert werden sollen. Dies wird bereits dann angenommen, wenn auf Websites bezahlte Werbung in Form von Bannern platziert wird.

Betreiber von Online-Shops auf Basis von Magento können mit dem kostenfreien Dienst MageReport überprüfen, ob ihr Shop-System bekannte Sicherheitslücken aufweist und von den aktuellen Angriffen betroffen ist. Zu jedem erkannten Problem werden detaillierte Informationen zu dessen Behebung bereitgestellt.

Bußgelder drohen

Das BSI weist explizit auf die Verpflichtungen aus § 13 Abs. 7 TMG hin. Dort heißt es:

> *"Diensteanbieter haben, soweit dies technisch möglich und wirtschaftlich zumutbar ist, im Rahmen ihrer jeweiligen Verantwortlichkeit für geschäftsmäßig angebotene Telemedien durch technische und organisatorische Vorkehrungen sicherzustellen, dass*
>
> *kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und*
> *diese*
> *a) gegen Verletzungen des Schutzes personenbezogener Daten und*
> *b) gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind,*
> *gesichert sind.*
> *Vorkehrungen nach Satz 1 müssen den Stand der Technik berücksichtigen. Eine Maßnahme nach Satz 1 ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens."*

Wer seine Systeme nicht schützt, begeht eine Ordnungswidrigkeit, die nach § 16 TMG mit einer Geldbuße in Höhe von bis zu 50.000 Euro geahndet werden kann.

Fazit

Online-Händler sollten dringend ihre Systeme überprüfen und entsprechende Sicherheitsupdates einspielen. Neben der Gefahr, mit einem Bußgeld belegt zu werden, droht natürlich auch ein riesiger Image-Verlust, wenn öffentlich wird, dass der eigene Online-Shop von diesen Angriffen betroffen und evtl. unzureichend dagegen geschützt war. (mr)

Bildnachweis: Sebastian Duda/shutterstock.com