Dolomiten
TAGBLATT DER SÜDTIROLER

Tiratura: 40.922 | **Diffusione:** 35.908 | **Readership:** 266.000
Data: 23/10/2026 | **Pagina:** 7
Categoria: Waren- und Dienstleistungsgenossenschaften Print & Web



Sicherheitslücken: Wer jetzt handeln muss

IT: Programmiersprache PHP betroffen – Einfallstor für Kriminelle – Vom Hotelauftritt bis zur Bürosoftware: Wie groß die Gefahr wirklich ist und was man tun kann

BERLIN (dpa/gam). Gravierende Sicherheitslücken in der weit verbreiteten Programmiersprache PHP versetzen IT-Sicherheitsexperten in Alarmbereitschaft. Betroffen sein können auch Websites und Webanwendungen in Südtirol. Doch wie groß ist die Gefahr wirklich und was ist nun konkret zu tun? Die wichtigsten Fragen und Antworten im Überblick.



Neu entdeckte, schwerwiegende Sicherheitslücken bringen das Fundament zahlreicher Webseiten und Onlinedienste ins Wanken. Betroffen ist die Programmiersprache PHP, auf der ein Großteil des gesamten Internets basiert – von einfachen Blogs über große Nachrichtenportale bis hin zu komplexen Onlineshops.

APA/afp/KIRILL KUDRYAVTSEV

Was genau ist passiert?
In der weit verbreiteten Programmiersprache PHP, auf der ein Großteil aller Webseiten basiert, wurden zwei extrem kritische Schwachstellen entdeckt (die „Dolomiten" haben berichtet). Sie erlauben es Kriminellen, aus der Ferne eigenen Schadcode auf Servern auszuführen. Mit anderen Worten: Angreifer können die vollständige Kontrolle über eine Website übernehmen, sensible Datenbanken und Kundendaten abgreifen oder sie für weitere Cyberattacken missbrauchen.

Behörden und IT-Sicherheitsexperten sprechen von einem außerordentlichen Notfall. Einige Webseitenbetreiber haben ihre Internetauftritte deshalb vorsorglich vom Netz genommen.

Ich habe eine Webseite, auf der ich meinen Betrieb vorstelle. Was muss ich tun?
In größeren Betrieben wird sich die hausinterne IT-Abteilung um das Problem kümmern. Kleinere Betriebe oder auch Vereine hingegen können selbst nicht allzu viel tun – außer sich an den Dienstleister wenden, der ihre Website betreut. Das kann eine Webagentur oder ein IT-Fachmann sein. Auch der Hosting-Anbieter, auf dessen Server die Seite liegt, kann zuständig sein.

„Denn ein kleiner Betrieb kann oft gar nicht wissen, ob seine Webseite auf PHP basiert – egal ob er sich die Webseite selbst auf einer Onlineplattform gebaut oder sie bei einem lokalen Anbieter bestellt hat", erklärt Stefan Laimer, Sicherheitsexperte der Konverto AG. Tätig werden müssen deshalb vor allem die Anbieter: „Sie sind nun gefordert, ihre eigenen Webseiten und jene, die sie den Kunden bereit stellen, zu überprüfen."

Wenn eine Webseite betroffen ist, muss die korrigierte PHP-Version installiert werden. Bei älteren Software-Versionen kann hingegen ein Wechsel auf eine neuere Version notwendig sein.

Ist eine rasche Absicherung nicht möglich, sollte geprüft werden, ob das betroffene System vorübergehend vom Netz getrennt werden muss. „Das wird sicher auch einige in Südtirol betreffen und hat natürlich größere Auswirkungen auf die Produktivität der Unternehmen", sagt Laimer.

Er betont auch, dass es nicht nur um Webseiten gehe: „Auch viele andere Webanwendungen, die ein Betrieb nutzt, können betroffen sein, zum Beispiel Bürosoftware, Webmail, Buchungssysteme oder die Bedienoberflächen von Firewalls und Netzwerkspeichern. Viele Anwendungen, die über den Browser laufen, basieren im Hintergrund auf PHP und könnten daher angreifbar sein."

Auf meiner Webseite gibt es keine Zahlungsmöglichkeiten, also auch keine sensiblen Daten. Muss ich mir dennoch Sorgen machen?
Wenn eine Webseite zum Beispiel eine reine Werbeseite für ein Hotel ist und keine Kundendaten oder Zahlungsinformationen speichert, ist der Schaden im Falle eines Angriffes womöglich zwar geringer. Aber auch dann haben Kriminelle Möglichkeiten, die Website zu kompromittieren. „Es könnte zum Beispiel passieren, dass die Seite für böswillige Zwecke weiterverwendet wird, um die nächsten Systeme anzugreifen oder um Besuchern Schadsoftware oder gefälschte Seiten unterzuschieben", erklärt IT-Experte Laimer.

Wie schnell müssen IT-Dienstleister handeln?
„Sehr schnell", sagt Laimer. „Das Update muss nun so schnell wie möglich installiert werden, weil leider auch die Angreifer sehr schnell sind." Auch bei Konverto sei man schon intensiv dabei, die Webseiten der Kunden zu kontrollieren.

Ich habe meine persönlichen Daten auf Online-Portalen eingegeben und in Onlineshops eingekauft – sind diese Daten nun in Gefahr?
Indirekt besteht ein Risiko. Wenn eine Website, ein Bürgerportal oder ein Onlineshop die betroffene PHP-Version nutzt und nicht rechtzeitig geschützt wurde, können Angreifer über den Schadcode Zugriff auf die dahinterliegenden Datenbanken erlangen. Dadurch könnten sensible Kundendaten, Passwörter oder Kontaktdaten abfließen.

Auf den Endgeräten der Nutzer selbst (wie Smartphones, Tablets oder PCs) besteht jedoch keine direkte Gefahr; die Schwachstelle liegt ausschließlich auf den Servern der Webseitenbetreiber im Hintergrund.

Wie geht es jetzt weiter und wann ist die Gefahr gebannt?
Weltweit hat es Experten zufolge schon Millionen Versuche von Hackern gegeben, die Schwachstellen auszunutzen. Und diese Welle automatisierter Angriffe werde voraussichtlich noch über Wochen und Monate hinweg andauern, da die Angreifer unermüdlich nach ungepatchten Systemen suchen. Entwarnung kann erst gegeben werden, wenn die breite Masse der Webhoster und Systemadministratoren die Sicherheitsupdates eingespielt hat.

© Alle Rechte vorbehalten

Ritaglio ad uso esclusivo del destinatario, è vietata la riproduzione e la distribuzione.