Newsletter 01/2025

FOX Group

Hat es mich erwischt? „Have I been pwnd“?

In der Welt des Datendiebstahls nutzen Unternehmen die Webseite des Australiers Troy Hunt, ob personbezogene Daten durch Datenlecks kompromittiert wurden. In der Regel mit der E-Mail-Adresse und der Telefonnummer. Über die Registrierung können Nutzer zusätzlich benachrichtigt werden, wenn Daten in zukünftigen Cyberattacken betroffen sind: die Website heißt: „have i been pwned.com“. Im Grunde eine gute Sache. Gibt es einen Haken? Wir sagen: „Ja“

Zwei Aspekte sind zu bedenken: Eine Geschäftsleitung von Webseiten und Internetdienstleistungen kann innerhalb kurzer Zeit wechseln, zuletzt gesehen bei Twitter. Was vorher vertrauenswürdig war, kann sich schnell zu einer Datenkrake entwickeln. Zusätzlich ist zu beachten, dass in Australien die Rechte von EU-Bürgern nur schwer durchzusetzen sind. Wer als Privatperson den Dienst nutzt, sollte wissen, dass die persönlichen Daten und ggf. auch das Passwort von einem Cyberangriff dieser Webseite betroffen sein können.

Wer nicht darauf verzichten mag, findet im „Leak Checker“ der Universität Bonn oder des Hasso-Plattner-Instituts in Potsdam mögliche Alternativen.

IT-Sicherheitsanforderungen Ihrer Webseite

In regelmäßigen Abständen erhalten unsere Datenschutz-Mandatskunden einen Auszug unserer Webseiten-Scans ihres Internetauftritts mit aktuellen Hinweisen, um sich auch vor möglichen Cyberangriffen zu wappnen. Meist sind die Datenschutzhinweise aus den Scans verständlich und für die Weitergabe an den Webdesigner und der Marketingabteilung ansprechend gestaltet.

Eine Rubrik weist auf den Umgang mit der X-Frame Option und der HSTS-Abfrage hin. Mit diesem Hinweis sind Webdesigner in der Regel anfänglich überfordert. Daher gehen wir heute auf das Thema ein:

Https//-Webseiten sind ausschließlich verschlüsselt im Internet zu finden. Wird sie unverschlüsselt als „http“ aufgerufen, wird der Nutzer umgehend auf die verschlüsselte HTTPS-Version weitergeleitet. Mit einer Man-in-the-Middle-Attacke kann ein Angreifer dies verhindern. Der Austausch zwischen Nutzer und Webseite lässt sich abfangen oder sogar auf eine gefälschte Version der Seite via HTTP umleiten.
Was fehlt ist ein Befehl an den Webbrowser, dass die aufgerufene Seite nur als HTTPS besucht werden kann. Wenn dieser Befehl nicht weitergegeben wird, kann die Seite ein Sicherheitsrisiko für den Betreiber darstellen.

Mit dem Html-Code „iFrames“ lassen sich Inhalte anderer Webseiten (z.B. Videos, Landkarten oder Dokumente) nahtlos in die eigene Webseite einbinden, ohne den Besucher auf diese Webseiten weiterleiten zu müssen. Ein „iFrame“ agiert wie ein Fenster mit Blick auf bestehende Internetportale. Im Grunde eine feine Sache.

Ein „iFrame“ lässt sich unbemerkt für Betrugszwecke nutzen. Platziert man z.B. transparente „iFrames“ über Eingabefelder einer Webseite, können so sensible Daten abgegriffen und an Betrüger weitergeleitet werden.

Mit einem X-Frame Option Header Befehl lässt sich das verhindern. Kontaktieren Sie hierzu Ihren Webdesign-Dienstleister.

Datenschutz und Informationssicherheit, ein Rück- und Ausblick

Auch im Jahr 2024 hat der Branchenverband Bitkom wieder Unternehmen zum Thema Wirtschaftsschutz befragt und in einer Studie zusammengefasst. Demnach sind 74 % der befragten Unternehmen von Datendiebstahl betroffen gewesen. Der Gesamtschaden durch kriminelle Handlungen stieg auf 266,6 Milliarden Euro. Der Schaden durch Cybercrime allein beträgt 178,6 Milliarden Euro. Der Täterkreis ist in der organisierten Kriminalität zu finden sowie in China und Russland. Zulieferer stellen sich hierbei immer mehr als Schwachstelle heraus, was von 44 % der befragten Unternehmen bestätigt wurde. Im Kampf gegen Cyberangriffe stufen 53 % der Befragten ihr eigenes Unternehmen dabei als gut aufgestellt ein. Ransomware spielte die Hauptrolle, gefolgt von Phishing-Angriffen und der Angriff auf Passwörter.

Der immer größere Einsatz von Künstliche Intelligenz (KI) verschärft die Bedrohungslage, davon gehen 83 % der Unternehmen aus. KI kann den Schutz aber auch deutlich verbessern, dieser Meinung sind 61 % der Unternehmen.

Auch das BSI bestätigt dieses Bild in seiner Untersuchung *„DIE LAGE DER IT-SICHERHEIT IN DEUTSCHLAND 2024“* und geht davon aus, dass der Einsatz von KI im hybriden Ansatz der Cyberkriminellen eine größere Rolle im Jahr 2025 einnehmen wird. Dabei werden nicht nur Angriffe mit KI orchestriert, sondern durch weitere Vektoren ergänzt. Dazu zählen beispielsweise Deepfakes von Bild- und Tonaufnahmen, sowie Desinformation zur Beeinflussung und Manipulation von Kunden, Lieferanten, Mitarbeitenden und Interessenten durch Social Bots. Die geopolitischen und zwischenstaatlichen Konflikte erhöhen die Bandbreite an Phänomenen im Cyberraum noch. Desinformation, Hacktivismus, Spionage und Sabotage werden hier vom BSI hervorgehoben.

Das Fazit für 2025: KI wird Angreifern die Möglichkeit geben, verfeinerte Methoden einzusetzen, um besser auf die Bedürfnisse der Opfer eingehen zu können. Auf der anderen Seite bietet eine KI aber auch der Informationssicherheit die Möglichkeit, große Datenmengen schneller und gezielter zu analysieren, um den Schutz von personenbezogenen Daten weiter zu gewährleisten. Daher empfiehlt es sich, die Informationssicherheit auf den Prüfstand zu stellen.

Studie: https://www.bitkom.org/sites/main/files/2024-08/240828-bitkom-charts-wirtschaftsschutz-cybercrime.pdf

BSI: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.pdf?__blob=publicationFile&v=5

Impressum

complimant AG, Edt 4, 84558 Kirchweidach

Vorstand: Franz Obermayer, Ann-Karina Wrede

Vorsitzender des Aufsichtsrates: Christian Volkmer

Telefon: +49 8683 99390-40

E-Mail: info@complimant.de / datenschutz@complimant.de

www.complimant.de

Eintragung im Handelsregister: Amtsgericht: Traunstein

Registernummer: HRB 20500 Steuernummer: 141/120/07009

Umsatzsteuer-Identifikationsnummer gemäß §27a

Umsatzsteuergesetz: DE274380239

Verantwortlich für den Inhalt nach § 55 Abs. 2 RStV Franz Obermayer