Nevis Security AG

26.10.2022 – 09:15 Uhr

Nevis Sicherheitsbarometer: Security-Profis schätzen Nutzer falsch ein

Zürich (ots) -

Cyberangriffe sind und bleiben ein massives Problem. Entsprechend essenziell ist es, dass sich Unternehmen und Kunden auf die wachsenden Gefahren einstellen und effektive Maßnahmen ergreifen. Mit dem Nevis Sicherheitsbarometer geht der Schweizer Spezialist für sichere Login-Lösungen der Stimmung im Bereich IT-Security auf den Grund. Die Resultate der aktuellen Studie zeigen, dass hier noch einiges zu tun ist. Besonders auffällig sind die Diskrepanzen zwischen den Erwartungen der Kunden und der Sicht der Unternehmen - sowie nicht zuletzt das Wissensdefizit der IT-Entscheider.

Für das Nevis Sicherheitsbarometer hat Nevis in Zusammenarbeit mit den Meinungsforschungsunternehmen Civey und mo'web research im Juli und August dieses Jahres 500 deutsche IT-Entscheider und 1.000 deutsche Konsumenten ab 14 Jahren zu Themen wie Passwortsicherheit und Loginverhalten online befragt.

Zahlreiche Gefahrenquellen

Dass die Zahl der Cyberangriffe kontinuierlich wächst, bekommen Unternehmen deutlich zu spüren: Werden ihre Datenbestände von Hackern angegriffen, drohen neben den direkten materiellen Einbußen - wenn etwa Gelder illegal transferiert werden - oft auch ein enormer öffentlicher Vertrauensverlust und die Abwanderung von Kunden. Dass die Gefahr wächst, sieht auch die Mehrzahl der für das Nevis Sicherheitsbarometer befragten IT-Entscheider so: Rund 57 Prozent gaben an, im letzten Jahr in ihrem beruflichen Umfeld einen Anstieg der Cyberkriminalität wahrgenommen zu haben; 39 Prozent sehen eher ein gleichbleibendes Niveau. 54 Prozent der IT-Profis erklärten zudem, dass ihr eigenes Unternehmen innerhalb der letzten 12 Monate Opfer einer Cyberattacke wurde. Dabei lässt sich nach ihren Angaben ein Viertel (26 Prozent) der registrierten Angriffe dem Bereich Ransomware zuordnen. Auf den weiteren Plätzen folgen Denial of Service (DoS) mit 20 Prozent, Brute-Force-Angriffe (18 Prozent) und Social Engineering (17 Prozent). Auffallend ist die mit 6 Prozent relativ seltene Nennung von Credential Stuffing - hier ist von einer hohen Dunkelziffer auszugehen, da bei dieser Angriffsvariante gestohlene Login-Daten zum Einsatz kommen, wodurch sie oft über lange Zeit unentdeckt bleibt.

Dass Unternehmen nicht immer optimal reagieren, wenn sie einen Angriff auf ihre EDV-Systeme entdecken, lässt sich an den Ergebnissen der Verbraucherbefragung ablesen: Gesetzlich sind Firmen in der Pflicht, ihre Kunden umgehend über Sicherheitspannen und mögliche Folgen zu informieren. Tatsächlich geben aber lediglich 41 Prozent der von einer Cyberattacke betroffenen Konsumenten an, dass sie durch das Unternehmen davon in Kenntnis gesetzt wurden - eine deutliche Verschlechterung der Informationslage gegenüber dem letzten NevisSicherheitsbarometer, bei dem es noch 48 Prozent waren. Dagegen scheint das Thema in den Medien mittlerweile deutlich häufiger aufgegriffen zu werden: 34 Prozent der Betroffenen erklärten, aus dieser Quelle vom Verlust ihrer Daten erfahren zu haben. 2021 hatten dies lediglich 15 Prozent der Studienteilnehmer geäußert.

Informationsdefizite bei IT-Entscheidern

Eine erschreckende Tendenz ließ sich ebenfalls schon am Nevis Sicherheitsbarometer des Vorjahres ablesen: Bei vielen Unternehmen ist die Absicherung ihrer Daten längst nicht so gut, wie sie sein könnte - und auch der Informationsstand vieler IT-

Entscheider über die dafür notwendigen Verfahren könnte durchaus besser sein. Auch 2022 ist keine Verbesserung dieser kritischen Punkte erkennbar. Die meistgenannten Vorkehrungen sind nach wie vor das Vorschreiben von Mindestlängen für Passwörter (65 Prozent) und die Verpflichtung zu regelmäßigen Passwortänderungen (41 Prozent). Auf die Zwei-Faktor-Authentifizierung per SMS setzen lediglich 34 Prozent; auf eine biometrische Zwei-Faktor-Authentifizierung nur 21 Prozent. Besonders erschreckend: rund 10 Prozent der befragten IT-Verantwortlichen geben an, keine Vorkehrungen für erhöhte IT-Sicherheit zu treffen. Und wenn es um Cybersecurity-Standards wie FIDO, Oauth oder WebAuthn geht, zeigt sich gerade einmal die Hälfte der Befragten mehr oder weniger gut informiert. Die andere Hälfte (47 Prozent) ist nach eigenem Bekunden mit keinem einzigen der gängigen Standards vertraut.

Die Gefahren aus Kundensicht

Und wie ist es auf Verbraucherseite um das Gefahrenbewusstsein in puncto IT-Sicherheit bestellt? Hier zeigt das Nevis Sicherheitsbarometer: Die Angst vor Cyberattacken und die Sorge um persönliche Daten ist unvermindert groß. Lediglich 5 Prozent der Befragten zeigen sich bezüglich der Sicherheit ihrer Daten absolut unbesorgt. Im Vergleich zum Vorjahr sind die Werte hier praktisch unverändert geblieben.

Wovor fürchten sich die Verbraucher konkret? Rund 68 Prozent sehen im Missbrauch der persönlichen Daten die größte Gefahr. Mit jeweils 59 Prozent ebenfalls weit oben in der Gefahrenliste sind die Angst vor Internetbetrug sowie die Angst, dass ein Fremder die persönlichen Internetkonten übernimmt. Die Bedenken gegenüber staatlicher Überwachung sind demgegenüber weniger stark ausgeprägt. Nur 28 Prozent der Befragten sehen darin eine Gefahr - eine Abnahme um sieben Prozent im Vergleich zur letzten Ausgabe des Nevis Sicherheitsbarometers.

Gleichzeitig nehmen es private Nutzer mit der Sicherheit nicht immer so genau, wie es eigentlich wünschenswert wäre: Im Rahmen der Befragung gaben 54 Prozent an, ein und dasselbe Passwort für mehrere Online-Konten zu verwenden - für Security-Experten ein absolutes No-Go. Trotz solcher Nachlässigkeiten ist sich die Mehrzahl über die Grundlagen der Passwortsicherheit durchaus im Klaren: 59 Prozent nutzen besonders komplexe Passwörter, die von Hackern nicht einfach erraten werden können, und immerhin 44 Prozent verwenden verschiedene komplexe Passworte für unterschiedliche Konten. Noch ausbaufähig ist die Nutzung moderner Sicherheitsverfahren: So greifen nur 34 Prozent auf die besonders sichere Zwei-Faktor-Authentifizierung zurück, um sich in ihre Konten einzuloggen; bei der biometrischen Authentifizierung - beispielsweise via FaceID oder Fingerbadruck - sind es sogar nur 17 Prozent. Dass dies nicht zuletzt daran liegt, dass viele Unternehmen diese Verfahren noch nicht im Einsatz haben, zeigt der Vergleich zwischen Kundenerwartungen und der Einschätzung durch die IT-Profis.

Unterschiedliche Erwartungen bei Kunden und Unternehmen

Für die Dienstleister im Internet ist es ein Dilemma: Ihre Kunden mögen selbst in puncto IT-Sicherheit noch Nachholbedarf haben, an die Unternehmensseite stellen sie aber hohe Erwartungen in Bezug auf Datenschutz und Cybersecurity - Erwartungen, die die Unternehmen nicht immer erfüllen. Besonders ins Auge fällt das beim Thema Zwei-Faktor-Authentifizierung: Während nur 4 Prozent der IT-Experten davon ausgehen, dass Kunden sich eine Zwei-Faktor-Authentifizierung (2FA) zur Konten-Absicherung wünschen, sind es tatsächlich 64 Prozent! Nicht zuletzt würden sich 45 Prozent der befragten Konsumenten sicherer fühlen, wenn ihre biometrischen Daten zum Login genutzt würden - dagegen gehen 57 Prozent der IT-Verantwortlichen davon aus, dass auf Kundenseite nur eine geringe Bereitschaft zur Nutzung dieses besonders sicheren Verfahrens bestehe.

"Wie schon im Nevis Sicherheitsbarometer des Vorjahres beobachten wir große Diskrepanzen zwischen dem Sicherheitsbedürfnis der Nutzer und den Annahmen, die IT-Verantwortliche über dieses Sicherheitsbedürfnis hegen", erklärt Stephan Schweizer, CEO der Nevis Security AG. "Diese Kluft gilt es zu überwinden, wenn Unternehmen das Vertrauen ihrer Kunden langfristig erhalten und gleichzeitig ihre Datenbestände effektiv schützen wollen. Die Werkzeuge, mit denen sich die IT-Security auf den neuesten Stand bringen lässt, sind vorhanden und einsatzbereit. Softwarebasierte Customer Identity und Access-Management-Systeme bilden hier den neuen Standard. Dabei gehört der passwortfreien Authentisierung die Zukunft - die großen Player wie Apple, Google und Microsoft arbeiten aktiv daran, den Loginprozess ohne Passwörter umzusetzen und ihn damit sicherer und komfortabler zu machen."

Das Nevis Sicherheitsbarometer steht unter folgendem Link zum Download bereit: https://www.nevis.net/de/nevis-sicherheitsbarometer

Pressekontakt:

Pressekontakt
LEWIS Communications GmbH
Ingo Geisler
Johannstraße 1
40476 Düsseldorf
+49 (0)211 882 476 07
nevis-security@teamlewis.com

Medieninhalte

Nevis Sicherheitsbarometer: Repräsentative Umfrage unter Verbrauchern und IT-Entscheidern zum Stand der IT-Security / Weiterer Text über ots und www.presseportal.de/nr/157549 / Die Verwendung dieses Bildes für redaktionelle Zwecke ist unter Beachtung aller mitgeteilten Nutzungsbedingungen zulässig und dann auch honorarfrei. Veröffentlichung ausschließlich mit Bildrechte-Hinweis.