Cyber-Stalking: Psychoterror aus dem Internet abwehren - ESET-Sicherheitsexperten schlagen Alarm und geben Anwendern Tipps zum Schutz ihrer Privatsphäre

Cyber-Stalking war noch nie so weit verbreitet wie heute. Es ist leicht, Menschen im digitalen Raum auszuspähen, zu analysieren und zu verfolgen. Doch vielen Internetnutzern fehlt noch immer die Sensibilität, um ihre Privatsphäre aktiv gerade in den sozialen Netzwerken zu schützen und so kein leichtes Ziel für Stalker zu sein. Fotos, Videos und Daten mit genauen Orts- und Zeitangaben werden arglos in sozialen Medien gepostet. Es gibt sogar so unbedarfte Anwender, die in Echtzeit ihre Standortdaten mit ihren Followern teilen. Nutzer lassen sich dadurch fast lückenlos tracken. Stalker können mit diesen Daten mühelos ganze Bewegungsprofile erstellen und dem Opfer jederzeit auflauern. In seinem aktuellen Blog-Artikel berichtet der ESET Sicherheitsexperte Jake Moore von alarmierenden persönlichen Erfahrungen und gibt Tipps für einen besseren Schutz der eigenen Privatsphäre.
"Während meiner Zeit als IT-Forensiker der britischen Polizei konnte ich verfolgen, wie weit Stalker gegangen sind, um ihre Opfer zu belästigen und zu peinigen", so Jake Moore, ESET Security Specialist. "Ich habe Berichte und Datensätze gelesen, die nicht nur beängstigend waren, sondern in einigen Fällen sogar tödlich endeten."
Cyber-Stalking bedarf dabei auf Seiten der Täter leider kein hohes technisches Know-how oder umfangreiche Spionage-Tools. Die effektive Nutzung Sozialer Netzwerke reicht häufig vollkommen aus. "Cyber-Stalking muss stärker in den gesellschaftlichen Fokus rücken", fordert zudem Thomas Uhlemann, ESET Security Specialist DACH. "Um Internetnutzer umfassend auszuspähen, bedarf es keines technischen Wissens. Anwender sollten in den sozialen Netzwerken, genau wie im echten Leben, stets misstrauisch sein und ihre Privatsphäre schützen."

Tipps für mehr Sicherheit in den sozialen Netzwerken

- Persönliche Daten schützen: Geben Sie nur Daten, Fotos oder Videos von sich preis, die sie theoretisch allen Internet-Nutzern mitteilen würden. Das Web ist wie eine grosse Pinnwand und darauf kann jedes Mitglied zugreifen, ohne Eingangskontrolle.

- Privatsphären-Schutz aktivieren: Viele Plattformen, wie Facebook, Instagram und Co., bieten Einstellmöglichkeiten für die Privatsphäre. Nehmen Sie sich die Zeit und richten Sie diese nach ihren persönlichen Bedürfnissen ein. Verlassen Sie sich auf keinen Fall auf die Standardeinstellungen.

- Prüfen Sie Kontaktanfragen genau: Immer wieder stellen unbekannte Mitglieder in sozialen Netzwerken Kontaktanfragen. Bleiben Sie misstrauisch, auch wenn vielleicht ein gemeinsamer Freund besteht, womöglich hat ihr bereits bestehender Kontakt unbedarft der Anfrage des Fremden zugestimmt. Erkundigen Sie sich ausserhalb der sozialen Netzwerke wenn möglich nach der Glaubwürdigkeit. Die Regel sollte aber lauten: Im Zweifel ablehnen!

Ungenutztes Konto löschen: Wenn Sie ein Konto in einem sozialen Netzwerk nicht mehr nutzen, sollten Sie es löschen. Häufig ist diese Funktion versteckt. Gründe für den Austritt müssen Sie nicht nennen, auch wenn bei einigen Plattformen eine Aufforderung erscheint.

- Kinder über Gefahren aufklären: Viele Kinder und Jugendliche sind sich häufig gar nicht bewusst, welche Gefahren in sozialen Netzwerken lauern. Der Spass geht ihnen meistens vor Sicherheit. Eltern sollten hier Interesse zeigen und mit den Kindern reden. Das stärkt ihre Medienkompetenz und schafft Vertrauen.