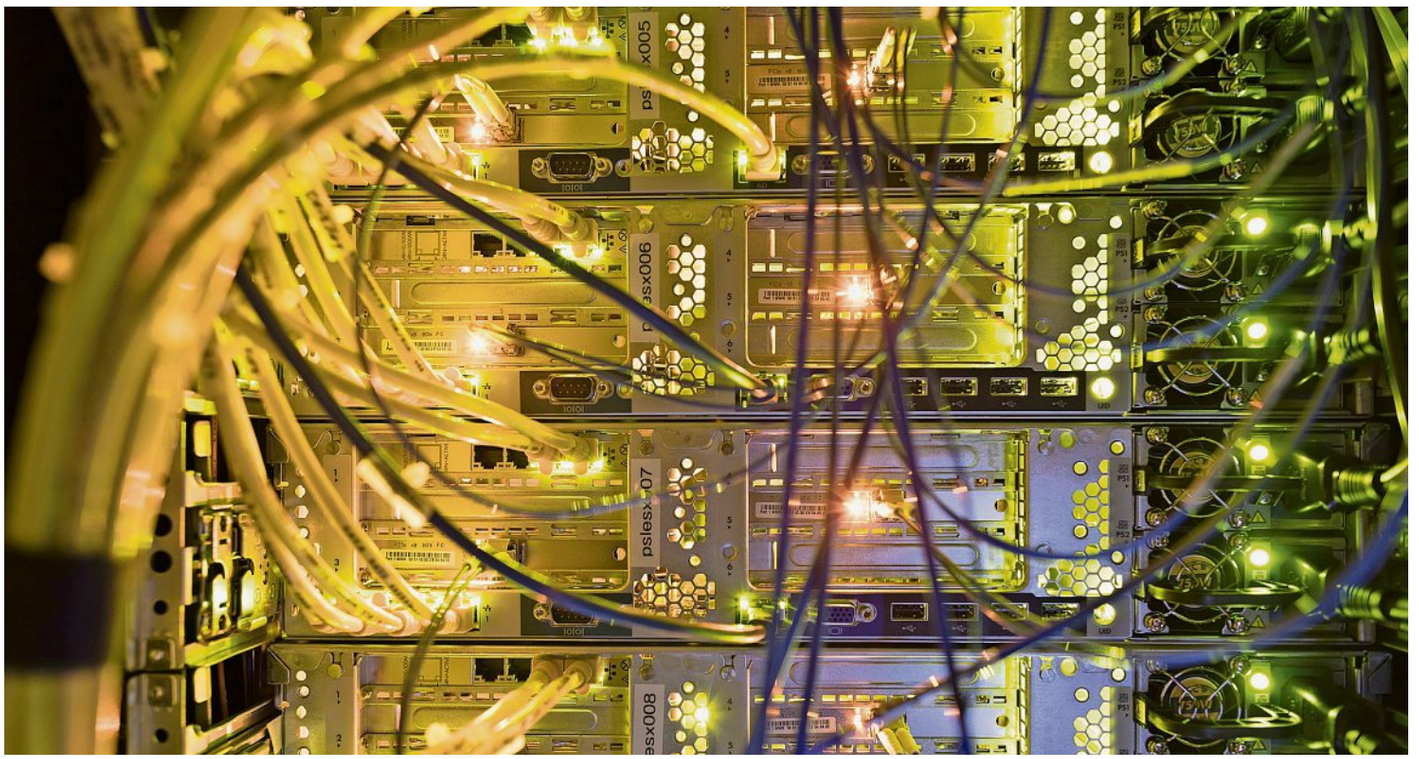
# Den kriminellen Hackern zuvorkommen

**Bug-Bounty-Programme** Die Cyberattacken häufen sich – auf Basler Schulen, eine Vormundschaftsbehörde im Wallis und die NZZ. Dagegen hilft der Einsatz von sogenannten ethischen Hackern. Der Bund macht es vor.

**Iwan Städler**



Wer sich mit dem Internet verbindet, geht ein Risiko ein. Sogenannte ethische Hacker können es senken. Foto: Gaëtan Bally (Keystone)

Nun hat es also auch die Basler Schulen erwischt: Noten, Absenzen und Abklärungsberichte sind seit Dienstagabend im Darknet zugänglich. In diesem versteckten Teil des Internets, der nur mit einer Spezialsoftware zugänglich ist, hat die Erpresserbande Bianlian angeblich Daten im Umfang von 1,2 Terabyte publiziert. «Eine grosse Zahl von Personen im Kanton Basel-Stadt dürfte betroffen sein», so Bildungsdirektor Conradin Cramer.

Auch die NZZ machte gestern Schlagzeilen, weil eine Hackergruppe weitere Daten veröffentlichte, nachdem die Bande das Medienunternehmen angegriffen hatte. Dieselbe Gruppe hackte jüngst die Vormundschaftsbehörde der Walliser Gemeinde Saxon. Es wird also ungemütlich für Firmen und Institutionen mit IT-Schwachstellen. Das belegt auch der gestrige Bericht des Nationalen Zentrums für Cybersicherheit (NCSC). Im letzten Jahr sind dort insgesamt 34'527 Meldungen eingegangen.

## Suche nach Schwachstellen

Wer glaubt, für kriminelle Hacker nicht interessant zu sein, könnte sich schon bald täuschen. Denn die Banden suchen überall nach Schwachstellen und nehmen, was sie kriegen. Meist lassen sie Bots das Internet abchecken und schlagen dort zu, wo es am einfachsten ist.

Dagegen helfen können sogenannte ethische Hacker. Sie sollen den Kriminellen zuvorkommen und die Schwachstellen vorher entdecken. Eine Firma oder Institution lädt diese Spezialisten also geradezu ein, ihr IT-System legal zu attackieren. Und wenn die gutgesinnten Angreifer eine Sicherheitslücke ausmachen (auf Englisch: bug), erhalten sie eine Prämie (bounty). Man spricht daher von Bug-Bounty-Programmen.

Doch viele Schweizer Firmen zögern immer noch, Hacker auf ihre Systeme loszulassen. Obwohl ethische Hacker mit kriminellen Hackern nichts gemeinsam haben ausser dem Namen und ihren Fähigkeiten. Für das NCSC ist daher klar, dass es Bug-Bounty-Programme braucht, um die Sicherheit gewährleisten zu können. In der Nationalen Cyberstrategie, die im April verabschiedet wurde, ist ethisches Hacking ein Schwerpunkt.

Der Bund will dabei Vorbild sein. Er hat ein Bug-Bounty-Programm beschlossen, das möglichst viele Systeme der Bundesverwaltung umfassen soll. Dafür spannt er mit Bug Bounty Switzerland zusammen, dem hiesigen Marktführer in diesem Business.

21'090 Franken hat der Bund bisher für Bounties bezahlt – knapp die Hälfte davon anlässlich eines Pilotprogramms im Mai 2021 und den grösseren Rest seit der Lancierung des eigentlichen Programms Ende letzten Jahres. «Das NCSC ist mit dem bisherigen Ergebnis zufrieden und wird das Bug-Bounty-Programm weiter ausbauen», sagt Sprecherin Manuela Sonderegger.

Neben dem Bund arbeitet Bug Bounty Switzerland auch mit mehreren Kantonen und Gemeinden zusammen. Das Unternehmen versteht sich als Vermittlungsplattform zwischen ethischen Hackern und Firmen respektive Institutionen, die ihren Schutz verbessern möchten.

## «Strenge Spielregeln»

«Bei jedem Programm gibt es strenge Spielregeln», sagt Sandro Nafzger, CEO von Bug Bounty Switzerland. Zugelassen sind lediglich ausgewählte Hacker, die zuvor auf ihre Seriosität überprüft worden sind. Bezahlt werden sie nur, wenn sie eine Schwachstelle finden. Für kleinere Bugs gibt es ein paar Hundert Franken. Für kritische Schwachstellen, bei welchen man das System übernehmen kann, winken 5000 bis 10'000 Franken. Im Extremfall können es auch mal 30'000 Franken sein.

Oft seien die Firmen erstaunt, so Nafzger, wie schnell ethische Hacker Schwachstellen fänden – nicht selten innert Stunden. Denn die Teilnehmer solcher Programme haben es eilig. Kriegen doch nur jene eine Prämie, die eine Sicherheitslücke als Erste entdecken. Meist werden solche Schwachstellen auch gefunden. «Es ist ein absoluter Ausnahmefall, dass niemand fündig wird», sagt er. Sei ein System derart sicher, dass man länger nichts Grösseres entdecke, könne man die Prämie auch erhöhen. Damit steigt der Anreiz, dass die Hacker intensiver suchen. Gleichzeitig sinkt auf diese Weise das Risiko, dass später Kriminelle auf die Schnelle ein Eingangstor finden. Die Bounties sind also eine Art Versicherung, nur meist günstiger.

Die höchste Prämie, die der Bund im Rahmen seines Programms ausbezahlt hat, beträgt 1500 Franken. Das zeigt, dass es in der Schweiz schwierig ist, von ethischem Hacken zu leben. Dafür muss man schon sehr gut sein. Andere machen es als Nebenbeschäftigung oder wohnen in Ländern mit tieferen Lebenskosten. 70 Prozent der ausbezahlten Prämien von Bug Bounty Switzerland würden aber in der Schweiz bleiben, so Nafzger. Seine Firma beschäftigt inzwischen 20 Mitarbeitende und konzentriert sich auf das Betreiben der Vermittlungsplattform, das Managen der Programme und das Beraten der Kunden. Dank dieser Unterstützung sei es auch kleineren Firmen und Gemeinden möglich, ein Bug-Bounty-Programm durchzuführen. Oft findet man bei ihnen am ehesten Sicherheitslücken.

Sandro Nafzger, CEO von Bug Bounty Switzerland. Foto: PD

Vorerst sind es aber vor allem grössere Firmen wie die Post, Coop, Ringier und mehr als 15 Banken, die bei Bug Bounty Switzerland anklopfen. Andere fürchten sich noch davor, Hacker einzuladen. Aber Kriminelle kommen auch ohne Einladung.