



Medieninformation

Swiss Cyber Storm 2026: Von Shadow-IT zu künstlicher Intelligenz und Quantencomputing

Die Swiss Cyber Storm 2026 findet am 20. Oktober im Kursaal Bern statt. Im Mittelpunkt steht die Shadow-IT: wenn Mitarbeitende mit eigener Software und Hardware die offizielle IT-Politik umgehen, um ihre Arbeit zu erledigen – und was das für Sicherheit und Compliance bedeutet. Daneben werden weitere aktuelle Themen wie Quantencomputing und künstliche Intelligenz ausführlich behandelt.

Eich, 9. Juli 2026 – Am 20. Oktober findet im Kursaal Bern die Swiss Cyber Storm statt. Die IT-Security-Konferenz steht dieses Jahr unter dem Motto «Shadow IT». Wenn Mitarbeitende – aus echtem Interesse oder aus dem Wunsch heraus, ihre Arbeit trotz hinderlicher Vorgaben zu erledigen – auf nicht offiziell genehmigte und verwaltete IT-Lösungen zurückgreifen, kann das durchaus produktiv sein. Gleichzeitig birgt Shadow-IT jedoch erhebliche Risiken für Sicherheit und Compliance. Aus dieser Diskrepanz ergibt sich eine Dynamik, die so alt ist wie die Unternehmens-IT selbst und die bis heute ungelöst bleibt (mehr im Blogartikel von Christian Folini: <https://www.swisscyberstorm.com/blog/2026/03/30/shadow-it-the-server-under-the-desk/>).

Genau deshalb steht Shadow-IT in all seinen Facetten im Zentrum der Swiss Cyber Storm 2026. Darüber hinaus erhalten künstliche Intelligenz (nicht nur in Form von Shadow-AI) sowie weitere aktuelle Themen wie Quantencomputing breiten Raum.

Das Programm: von Quantencomputing über künstliche Intelligenz bis Shadow-IT

Das Programm der diesjährigen Konferenz nimmt Gestalt an. Im Folgenden eine Auswahl an Referenten, die ihre Erkenntnisse und aktuellen Forschungsergebnisse an der Swiss Cyber Storm 2026 vorstellen werden:

- **[Stéphane Adamiste](#)** (Soluss) präsentiert die Erkenntnisse aus seiner Prüfung des Schweizer E-Voting-Systems. Sein Vortrag führt durch die zahlreichen bisher veröffentlichten Berichte, insbesondere zu Infrastruktur und Betrieb. Adamiste ist Spezialist für Informationssicherheit und Datenschutz mit langjähriger Prüfungserfahrung in verschiedenen Branchen.
- **[Mazin Ahmed](#)** (FullHunt) ist Spezialist für Informationssicherheit und Penetrationstester. Er hielt einen Vortrag an der Swiss Cyber Storm 2016, als er noch Student im Sudan war und an Schweizer Bug-Bounty-Programmen teilnahm. Seitdem ist er nach Kanada gezogen und hat FullHunt gegründet, einen Dienst, der Unternehmen ein gross angelegtes Angriffsflächenmanagement bietet. In seinem Vortrag («Shadow IT as visible on the internet») wird Mazin Erkenntnisse aus der Schweiz vorstellen. Er wird unter anderem auf Server eingehen, die eigentlich nicht nach aussen hin zugänglich sein sollten.
- **[Marco Brenner](#)** (IBM Research) erläutert, warum IBM überzeugt ist, dass der Quantencomputer näher rückt – in nicht mehr als fünf bis zehn Jahren. Sein Vortrag steht unter dem programmatischen Arbeitstitel «Here are your next steps as the development is accelerating» und bietet konkrete, praxisnahe Handlungsempfehlungen. Brenners Einschätzung: Der gängige Ratschlag, zunächst ein Asset-Inventar aufzubauen, führt in eine Sackgasse.
- **[Andres Maurer](#)** (Prod) widmet sich dem Thema digitaler Betrug. Die FINMA hat im April entsprechende Leitlinien veröffentlicht, und das NCSC will in diesem weitreichenden Bereich, der die Bevölkerung direkt betrifft, wirksamer vorgehen. Maurer teilt Erfahrungen aus dem Inneren des Bankensektors.
- **[Sébastien Schnyder](#)** (Google) leitet ein Cyber-Threat-Intelligence-Team bei Google. Sein Vortrag trägt den Arbeitstitel «Adversarial uses of AI: a voyage along vibe coded kill chains» und beleuchtet, wie Kriminelle heute Cloud-basierte Sprachmodelle einsetzen. Hinweis: Dieser Vortrag

ist ausschliesslich für Teilnehmende der Swiss Cyber Storm 2026 bestimmt. Er wird weder aufgezichnet noch werden die Folien veröffentlicht.

- [Ivano Somaini](#) (Compass Security) spricht über Open-Source Intelligence (OSINT) im Zeitalter der künstlichen Intelligenz. Somaini ist Experte für offensive Sicherheit, Social Engineering und OSINT, verfügt über einen Informatikabschluss der ETH Zürich und langjährige praktische Erfahrung in Red-Team-Übungen. Sein OSINT-Fachwissen hat er unter dem ehemaligen FBI-Agenten Mike Bazell vertieft. 2024 gründete er OSINT Switzerland.
- [Jeroen van der Ham-de Vos](#) (Universität Twente) leitete das niederländische GovCERT, bevor er in die Wissenschaft wechselte. Er bewegt sich an der Schnittstelle von Technologie und Politik und ist eine treibende Kraft hinter DIVD, einer Organisation, die sich der verantwortungsvollen Offenlegung von Sicherheitslücken weltweit widmet. Im Mittelpunkt seines Vortrags stehen Schwachstellenmanagement und Shadow IT.
- [Tin Zaw](#) (Fastly) verfügt über jahrzehntelange Erfahrung im Bereich Unternehmenssicherheit und hat Initiativen bei Branchenführern wie Qualcomm, Symantec, AT&T, Intuit und Verizon geleitet. An der Swiss Cyber Storm 2026 wird er auf seine Erfahrungen als Projektleiter des Automated Threats Project zurückgreifen, das er seit 2015 mitleitet. Automatisierte Bedrohungen umfassen all die verschiedenen Probleme, die durch Bots entstehen, die Ihre Dienste nutzen – und das sind eine ganze Menge.

Zusätzliche Details zu weiteren Referenten, Vorträgen und der Konferenz werden zu gegebener Zeit auf der Website von Swiss Cyber Storm bekannt gegeben: <https://www.swisscyberstorm.com/schedule/>

Tickets für die Swiss Cyber Storm Conference 2026 können unter <https://pretix.eu/scs/2026/> bezogen werden.

Über Swiss Cyber Storm

Swiss Cyber Storm hat sich in den vielen Jahren ihres Bestehens als *die* IT-Security-Konferenz der Schweiz etabliert und setzt heute die Themen für die Schweizer Sicherheitsbranche. Am Event präsentieren internationale Koryphäen neueste Erkenntnisse einem vielschichtigen nationalen Publikum, das sich aus Studenten, Techies und IT-Security-Leitern zusammensetzt. Während an anderen Konferenzen gerne über Schwachstellen gesprochen wird, liefert Swiss Cyber Storm dazu den Kontext und präsentiert praktische und erprobte Lösungen für strukturelle Sicherheitsprobleme. www.swisscyberstorm.com

Kontakt Swiss Cyber Storm

Christian Folini
Program Chair

+41 79 220 23 76
christian.folini@swisscyberstorm.com