



Medieninformation

Swiss Cyber Storm 2026: US-Generalleutnantin (a. D.) Karen Gibson hält Eröffnungs-Keynote



US-Generalleutnantin (a. D.) / U.S. Lieutenant General (Ret.) Karen H. Gibson

Die Swiss Cyber Storm 2026 mit dem Fokusthema «Shadow-IT» findet am 20. Oktober im Kursaal Bern statt. Die Opening-Keynote hält Karen H. Gibson, US-Generalleutnantin (a. D.) und ehemalige Ordnungsbeauftragte des Senats der USA. Das Konferenzprogramm ist nun komplett und online verfügbar.

Eich, 06. Oktober 2026 – US-Generalleutnantin (a. D.) Karen H. Gibson hält die Eröffnungs-Keynote der Swiss Cyber Storm 2026. Karen Gibson war von 2021 bis 2025 die 42. Ordnungsbeauftragte des US-Senats. Sie wurde nach dem Angriff auf das Kapitol am 6. Januar ernannt und war als oberste Verantwortliche für Strafverfolgung, Protokoll und Sicherheit im Senat tätig. Unter ihrer Leitung wurden die Programme für physische Sicherheit, Regierungsführung und Cybersicherheit grundlegend überarbeitet, einschliesslich des Schutzes von 450 Senatsbüros in den gesamten Vereinigten Staaten.

Gibsons Keynote trägt den Titel: **«Seeing the Shadows: Securing What You Don't Control»**. Auf der Grundlage ihrer Erfahrungen mit der Absicherung aller Aspekte der Arbeitsabläufe im US-Senat und einer Karriere, die von militärischem Nachrichtendienst bis hin zu Cyberoperationen reicht, beleuchtet Gibson in ihrer Ansprache eine grundlegende Herausforderung für Cybersicherheitsverantwortliche: den Schutz dessen, was man nicht immer sehen oder kontrollieren kann. Von Altsystemen und veralteter Technologie bis hin zu Personalpraktiken und Abhängigkeiten von Drittanbietern untersucht sie, wie sich versteckte Schwachstellen ansammeln – und was Führungskräfte tun können, um Risiken besser zu verstehen, die Widerstandsfähigkeit zu stärken und den Auftrag zu schützen. Mehr Informationen über Karen Gibson finden Sie [hier](#).

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

Die Swiss Cyber Storm 2026 findet am 20. Oktober im Kursaal Bern 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. Daneben erhalten im diesjährigen Programm aber auch weitere aktuelle Themen wie künstliche Intelligenz oder Quantencomputing Raum.

Dies sind die Referenten, die ihre Erkenntnisse und aktuellen Forschungsergebnisse an der Swiss Cyber Storm 2026 präsentieren werden:

- [Stéphane Adamiste](#) prüft seit Jahren das E-Voting-System der Schweiz. Er wird seine wichtigsten Erkenntnisse vorstellen und die Sicherheit des Systems bewerten.
- [Mazin Ahmed](#) von Fullhunt.io hat speziell für uns die Angriffsfläche in der gesamten Schweiz untersucht. Dabei stiess er auf eine Vielzahl von Schatten-IT-Systemen.
- [Marco Brenner](#) arbeitet bei IBM an Quantencomputern – ein Thema, das nicht mehr weit in der Zukunft liegt, aber oft falsch angegangen wird.
- [Nadim Kobeissi](#) stellt seine Software „Verifpal“ vor und zeigt, wie sich damit komplexe Protokolle auch ohne fundierte Kenntnisse der Kryptografie analysieren lassen.
- [Felix Linker](#) arbeitet am digitalen Emblem des Roten Kreuzes, das darauf abzielt, die Online-Infrastruktur für Angreifer sichtbar und identifizierbar zu machen.
- [Hannes Lubich](#) ordnet verschiedene Formen von Schatten-IT in eine Taxonomie ein und erklärt, wie wir damit umgehen sollten.
- [Loïc Maréchal](#) hat die Cyber-Forschungslandschaft in der Schweizer Industrie untersucht. Er präsentiert seine Lückenanalyse und gewährt Zugang zu seinen Daten.
- [Andreas Maurer](#) konzentriert sich auf digitalen Betrug – ein Thema, das derzeit auch die FINMA beschäftigt. Hier stellt er sein „Trident Resilience Framework“ vor.
- [Michael Morgenstern](#) verfügt über neue Daten zu „Shadow AI“ in Unternehmen. Und er hat einige Ideen, wie man mit dem Problem umgehen könnte.
- [Benjamin Rothenberger](#) wird erläutern, wie das Post-Quantum-Problem die Art und Weise, wie Browser Verschlüsselung nutzen, grundlegend verändern wird. Die Veränderung muss über den blossen Austausch einiger Algorithmen hinausgehen.
- [Sébastien Schnyder](#) beobachtet Kriminelle bei der Arbeit mit Google-KI. Er veranschaulicht deren Vorgehensweise anhand konkreter Beispiele und erklärt, was wir daraus lernen sollten.
- [Ivano Somaini](#) ist Vorreiter, wenn es um den Einsatz von Technologie im Bereich OSINT geht. KI eröffnet völlig neue Wege. Er wird uns zeigen, wie.
- [Jeroen van der Ham-de Vos](#) verfügt über umfangreiche Erfahrung im Bereich Schwachstellenmanagement – ein Feld, das durch KI unter neuen Druck geraten ist. Was muss also getan werden?
- [Tin Zaw](#) nimmt den HTTP-Verkehr unter die Lupe und identifiziert Bot-Verkehr als „Schattenverkehr“. Ausserdem zeigt er auf, was man heute dagegen tun kann.

Die niederländische Verhaltensanalytikerin [An Gaiser](#) wird die Veranstaltung abschliessen und in ihrer Keynote verschiedene Aspekte von Deepfakes erörtern und eine der hartnäckigsten Vorstellungen der Cybersicherheit hinterfragen: dass der Mensch das schwächste Glied in der Kette sei. Sie hat einige provokante Theorien parat.

Das gesamte Konferenzprogramm steht zur Verfügung unter: <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