

Cyberkriminalität: Erfolgreiche Zerschlagung der IT-Infrastruktur einer Ransomware-Gruppe dank einer international koordinierten Aktion

2.10.2026 - | Eidgenössisches Departement für auswärtige Angelegenheiten EDA

Bern, 01.10.2026 — Am 30. September gelang es im Rahmen einer gross angelegten internationalen Operation, eine von der Ransomware-Gruppe «KillSec» genutzte IT-Infrastruktur zu zerschlagen. Das Bundesamt für Polizei fedpol und die Bundesanwaltschaft (BA) waren als operative und strategische Partner direkt an der Intervention beteiligt.

Die BA führt seit dem 31. Juli 2025 ein Strafverfahren gegen Unbekannt wegen unbefugter Datenbeschaffung (Art. 143 StGB), unbefugtem Eindringen in ein Datenverarbeitungssystem (Art. 143bis StGB), Datenbeschädigung (Art. 144bis StGB) und Erpressung (Art. 156 StGB) infolge von Ransomware-Angriffen, die von der Ransomware-Gruppe KillSec (oder «KillSecurity») zwischen Oktober 2023 und Juni 2025 gegen mehrere Schweizer Unternehmen verübt wurden.

Bei Ransomware-Angriffen dringt die Täterschaft unbefugterweise in das Datenverarbeitungssystem des Opfers ein, kopiert und entwendet relevante Daten, verschlüsselt anschliessend die Server und fordert dann ein Lösegeld als Gegenleistung für den Entschlüsselungscode. Das Lösegeld muss dabei häufig in einer Kryptowährung gezahlt werden. Wie andere Ransomware-Gruppen wendet auch KillSec die Angriffsmethode der «doppelten Erpressung» an. Das heisst, nachdem sie die Server des betroffenen Unternehmens verschlüsselt hat, droht die Täterschaft mit der Veröffentlichung dieser Daten im Darknet, sollte sich das Unternehmen weigern, das Lösegeld zu zahlen – beispielsweise, weil es die Daten vor deren Entwendung gesichert hat.

Im Rahmen dieses Strafverfahrens haben sich die BA und fedpol an den auf internationaler Ebene geführten Ermittlungen beteiligt, die von Europol und Eurojust koordiniert wurden, gemeinsam mit den Behörden aus sieben weiteren Ländern.

In diesem Zusammenhang wurde von den oben genannten europäischen Agenturen eine Abschaltaktion vorbereitet und am 30. September 2026 durchgeführt. Die Aktion führte zur Festnahme von drei Personen sowie zur Beschlagnahmung von Beweismitteln und Vermögenswerten.

In Spanien, Griechenland, dem Vereinigten Königreich und Rumänien wurden insgesamt acht Hausdurchsuchungen durchgeführt. Dabei konnten die Behörden mindestens 110 Terabyte gestohlener Daten sicherstellen. Insbesondere wurden fünf Server beschlagnahmt, die von der Gruppe zur Speicherung der Daten ihrer Opfer verwendet wurden.

Angesichts des internationalen Charakters der Cyberkriminalität ist eine enge Zusammenarbeit zwischen den verschiedenen Partnern auf nationaler und internationaler Ebene unerlässlich. Der Aktion gingen umfangreiche Ermittlungen voraus, die fedpol unter der Leitung der BA durchführte. In enger Zusammenarbeit mit den Kantonspolizeien und dem Bundesamt für Cybersicherheit (BACS) sammelten und analysierten die Ermittler von fedpol detaillierte Informationen über den Modus

operandi des Netzwerks. Wie auch die Staatsanwälte des Bundes koordinierten sie den Informationsaustausch mit den ausländischen Partnern und trugen somit auch zum Erfolg der Operation bei.

Die Bekämpfung der Cyberkriminalität zielt natürlich nicht nur auf die Identifikation der Täterschaft und deren Strafverfolgung, sondern auch auf eine Unterbindung ihrer Aktivitäten sowie die Zerschlagung ihrer Infrastrukturen ab. Die Beschlagnahme von Servern und Daten beeinträchtigt die Funktionsweise eines kriminellen Netzwerks und schränkt die Fähigkeit der Täterschaft, ihre kriminellen Aktivitäten fortzusetzen, ein. Zugleich ermöglicht sie das Sammeln neuer Beweismittel, die zur Identifizierung der Cyberkriminellen beitragen und ein besseres Verständnis der Rolle und des Beteiligungsgrads der verschiedenen Akteure ermöglicht.

Für alle Verfahrensbeteiligten gilt die Unschuldsvermutung. Die BA erteilt derzeit keine weiteren Auskünfte zum laufenden Strafverfahren.

Die BA und fedpol setzen ihre Ermittlungen trotz des Rückschlags für dieses Netzwerk von Cyberkriminellen fort. Die Behörden arbeiten weiterhin mit vollem Einsatz daran, die Täter von Cyberdelikten zu identifizieren, sie festzunehmen und – sofern sie sich im Ausland befinden und die Umstände es zulassen – ihre Auslieferung an die Schweiz zu erwirken, wie dies bereits in mehreren Fällen geschehen ist. Sie bemühen sich zudem um deren strafrechtliche Verurteilung.

In diesem Zusammenhang weist das BACS erneut darauf hin, wie wichtig es ist, Cyberangriffe zu melden und Strafanzeige zu erstatten, um so die Wirksamkeit der Ermittlungen zu stärken und generell zur Bekämpfung der Cyberkriminalität beizutragen. Alle – ob öffentliche Einrichtungen, Unternehmen oder Privatpersonen – nicht nur Unternehmen von strategischer Bedeutung, sind potenzielle Zielscheiben dieser Angriffe. Privatpersonen und Organisationen, die Opfer eines Cyberangriffs geworden sind, werden daher ermutigt, den Vorfall den zuständigen Behörden zu melden oder direkt bei der Polizei oder der Staatsanwaltschaft Anzeige zu erstatten.

Links

Ransomware
Bundesamt für Cybersicherheit

<https://www.eda.admin.ch/de/newsb/cBOoSTI5a7sc>