Cyber-Sicherheit: In der Direktion Staatsschutz und Nachrichtendienst arbeitet ein Expertenteam an der Aufklärung von Cyber-Angriffen und dem Schutz vor Cyber-Bedrohungen

Analysieren, auswerten, abwehren

Im Bereich Cyber-Sicherheit in der Direktion Staatsschutz und Nachrichtendienst arbeitet ein Expertenteam aus Ermittlern, IT-Security-Analysten und IT-Technikern daran, Cyber-Angriffe aufzuklären und abzuwehren, die gegen verfassungsmäßige Einrichtungen gerichtet sind

In den vergangenen Jahren sind die Anzahl und das Ausmaß von Cyber-Angriffen gestiegen. Nicht nur kleine Firmen ohne eigenes IT-Sicherheitsbudget fallen Kriminellen zum Opfer, sondern auch große Firmen und Organisationen wurden Opfer von Cyber-Kriminellen. Die Direktion Staatsschutz und Nachrichtendienst (DSN) analysiert Cyber-Angriffe und sensibilisiert Bedarfsträger hinsichtlich der potenziellen Gefahren. Aufgrund der digitalen Abhängigkeiten vieler Kernprozesse können Firmen durch Cyber-Angriffe beispielsweise in Konkurs getrieben werden, wichtige Informationen an ausländische Akteure verloren gehen oder Geschäftsbeziehungen zerbrechen.

Als Cyber-Sicherheitsbedrohungen werden Tätigkeiten von Akteuren gemessen, die sich das Ziel gesetzt haben, mithilfe digitaler Mittel Angriffe auf IT-Systeme zu setzen. Diese können sich durch die Unterbindung der Funktionalität von IT-Systemen auswirken, deren Überlastung (etwa in Form von DDoS-Angriffen) oder durch unterschiedliche Aktivitäten nach dem erfolgreichen Eindringen in Netzwerke. Beispiele sind Sabotagemaßnahmen durch die Manipulation von Daten oder der Diebstahl von Informationen, die für den Angreifer wichtig sind.

Cyber-Sicherheit. Die Mitarbeiterinnen und Mitarbeiter des *Cyber-Security-Centers (CSC)* der DSN sind zuständig für die Analyse von Angriffen durch terroristisch, ideologisch oder religiös motivierte, staatliche oder nachrichtendienstlich unterstützte Akteure gegen österreichische Interessen. Zudem steht der Schutz von verfassungsmäßigen Einrichtungen, von kritischer Infrastruktur und von internationalen Organisationen vor Cyber-Angriffen im Fokus ihrer Arbeit. Das *CSC* ist Kontaktstelle für Beratungen und Hilfestellungen für Firmen oder Organisationen bei Cyber-Angriffen, um Abwehrmaßnahmen zu verbessern.

In der DSN arbeitet ein Expertenteam an der Aufklärung von Cyber-Angriffen und dem Schutz vor Cyber-Bedrohungen. Oft wird davon ausgegangen, dass in Sicherheitsbehörden und Nachrichtendiensten nur technische Computerspezialistinnen und Computerspezialisten arbeiten, die Programmierkenntnisse haben. Doch bei diesen Bedrohungen handelt es sich um Querschnittphänomene mit Zusammenhängen und Auswirkungen außerhalb der

FOTOS: DSN, SIKOV - STOCK.ADOBE.COM

digitalen Welt, weshalb die Cyber-Expertinnen und -Experten in der DSN verschiedene Ausbildungshintergründe haben – von technisch spezialisierten Polizistinnen und Polizisten über Personen mit wirtschaftlichen und sozialwissenschaftlichen Studienabschlüssen bis hin zu Informationstechnikerinnen und Informationstechnikern sowie Forensikerinnen und Forensikern.

Rekonstruiert werden Installation und Ausführung von Schadsoftware auf IT-Systemen von technischem Fachpersonal, um die vorhandenen Rohdaten zu interpretieren und die Zusammenhänge darzulegen. Diese Analyse ist nur einer von vielen Schritten im sicherheitsbehördlichen Prozess. Weiters gilt es, die Vorgangsweise eines Angreifers zu verstehen. Deshalb kommen in der DSN neben den IT-Spezialistinnen und Spezialisten technische Analytikerinnen und Analytiker und Cyber-Ermittlerinnen und -Ermittler zum Einsatz.

Wie bei der Bearbeitung jedes anderen Phänomens im Verfassungsschutz benötigen die Cyber-Ermittlerinnen und -Ermittler grundlegendes Verständnis für die fachlichen Zusammenhänge und das verwendete Vokabular, jedoch haben sie einen weniger technischen Auftrag bei der Bekämpfung von Cyber-Angriffen als die Analytikerinnen und Analytiker.

Bei der polizeilichen Ermittlung geht es darum, Sachverhaltsdarstellungen nach einem Cyber-Angriff zu verfassen, rechtliche Maßnahmen mit der Staatsanwaltschaft abzuklären und die Maßnahmenplanung zu koordinieren. Das Internet macht nicht an den Landesgrenzen Halt, daher sind auch internationale Kommunikation und Informationsaustausch notwendig, um den strafprozessualen und gefahrenabwehrenden Tätigkeiten vollständig nachzugehen.

Bei den Cyber-Analytikerinnen und -Analytikern liegt der Fokus auf dem Auswerten von Berichten von vergangenen Angriffen der Bedrohenden, allerdings werden, basierend auf diesen Informationen, Gegenmaßnahmen zur Abwehr zukünftiger Angriffe geplant. Aufgrund der oft großen Datenmengen werden Data-Science-Analysen engagiert, um diese effizient zu verarbeiten und Erkenntnisse zur Bekämpfung von Cyber-Bedrohungen zu gewinnen. Da die gesamtstaatlichen Auswirkungen oder Einschätzungen von ausländischen Akteuren in strategische Analysen verfasst werden, sind Kommunikationsfähigkeit und Schreibkompetenz wichtig. Die Analytikerinnen und Analytiker vermitteln die Ergebnisse der Analyse an nicht technische Stakeholder. Ein polizeilicher Hintergrund ist nicht notwendig.

Die Abwehr von Cyber-Bedrohungen erfolgt im Verfassungsschutz aus Sicht der Ermittlung und Analyse mit einer interdisziplinären Herangehensweise, die technisches Wissen mit kriminalistischen Fähigkeiten und rechtlichem Verständnis kombiniert. Die Analytikerinnen und Analytiker analysieren Cyber-Angriffe und wehren diese ab, sammeln und bewerten digitale Beweise und identifizieren neue Bedrohungsphänomene. Eines eint das Expertenteam der DSN, das weiterhin im Bereich der Ermittlung und in der Analyse auf der Suche nach Unterstützung ist: die Faszination für die Cyber-Thematik.