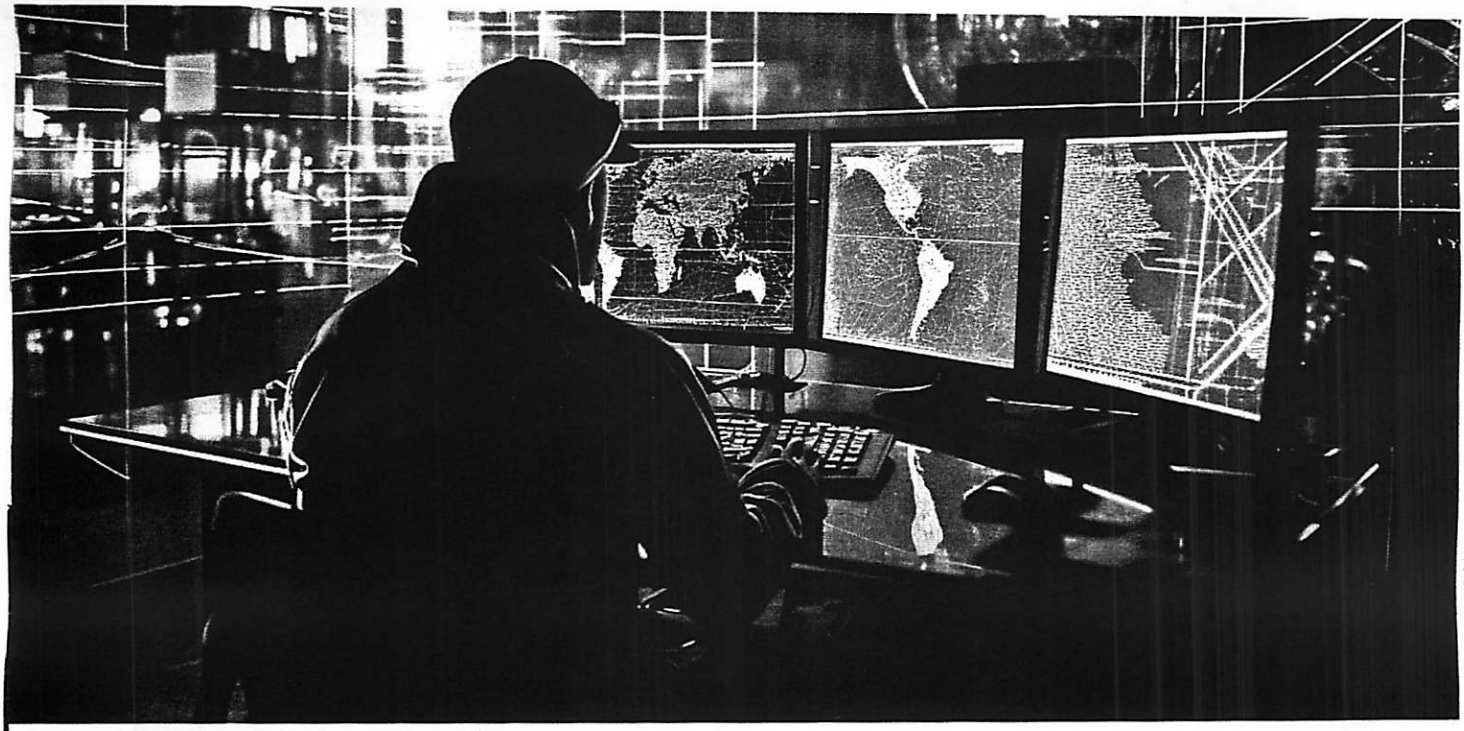

Fotos: Boris Bärmichl

Cyberkriminelle agieren wie „Firmen" mit entsprechenden Strukturen.

Das Tor zur Unterwelt

Die Cyberkriminalität wächst. Für Sicherheitsbehörden, Unternehmen und Organisationen ist es daher unerlässlich, ein Darknet-Monitoring durchzuführen.

BORIS BÄRMICHL

Das Darknet hat sich zu einem geheimen Ort für Cyberkriminelle entwickelt, die illegale Aktivitäten wie den Handel mit gestohlenen Daten, Drogen, Waffen und sogar Auftragsmorden betreiben. Um sich entsprechend zu schützen, muss das Darknet aktiv überwacht und analysiert werden.

Das Darknet ist ein Teil des Internets, der über spezielle Verschlüsselungstechnologien und anonymisierende Dienste zugänglich ist und es dem Anwender erlaubt, ebenso unerkannt unterwegs zu sein. Es bietet viele versteckte Plattformen für illegale Aktivitäten und ermöglicht den Nutzern, ihre Identität zu verschleiern. Durch die Verwendung von Kryptowährungen wie Bitcoin wird der Handel im Darknet noch weiter anonymisiert. Somit ist das Darknet das Netzwerk für geheime Dienstleistungen geworden, was Vor- (zum Beispiel für Journalisten) und große Nachteile für Behörden und Firmen hat.

Wie in der normalen Geschäftswelt

Cyber Crime ist zu einem sehr professionellen Geschäft geworden. Die Akteure haben eine Arbeitsteilung eingeführt, es gibt Gruppen wie zum Beispiel Lockbit, Conti, Alphv oder Hive, die im Darknet Partnerprogramme anpreisen wie in der ganz normalen Geschäftswelt. Hier kann sich der jeweilige Kriminelle entscheiden: Arbeitet er für die Abteilung Schwachstellen finden oder Ausnutzung von Schwachstellen, vielleicht ist auch mehr das Schadcode Installieren in den angegriffenen Netzwerken oder die Entwicklung und Anpassung von Schadcode sein Fall. Es gibt zudem ein Belohnungssystem mit Abstufungen in Bronze, Silber, Gold oder Platin – je nachdem wie gut der Kriminelle ist, wie viel der Angreifer umsetzen kann. Die gewonnen Informationen werden in diesen Gruppen ausgetauscht. So entsteht ein sehr professionelles und gut vernetztes Vorgehen. Preisgelder und Prämien sorgen dafür, dass immer mehr hoch motivierte Angreifer uns attackieren. Durch die Kryptowährungen hat das Cyber Crime seinen eigenen anonymen Bezahldienst etabliert und das Ganze ohne Buchhaltung und Steuern zu zahlen. Wenn wir an die Slums der Welt denken, sehen wir das mögliche „Mitarbeiter-Potenzial". Durch das Zur-Verfügung-Stellen von Computern an Jugendliche in ärmlichen Verhältnissen ziehen sich Kriminelle die nächste Generation von Cyberkriminellen heran.

> „Wenn wir an die Slums der Welt denken, sehen wir das mögliche ‚Mitarbeiter-Potenzial' des Cyber Crime."
>
> **Boris Bärmichl,** Vorstandsmitglied des BVSW e.V.

Überwachung immer wichtiger

Darknet-Monitoring und -Analyse bekommen so eine ganz neue Bedeutung. Aus der Risikobetrachtung heraus wird sehr schnell klar: Durch das Überwachen des Darknets können Sicherheitsbehörden und Unternehmen frühzeitig potenzielle Bedrohungen erkennen und proaktiv Maßnahmen ergreifen lassen, um Angriffe zu verhindern oder einzudämmen. Darknet-Monitoring und -Analyse ermöglichen es, illegale Aktivitäten wie den Handel mit gestohlenen Daten, gehackten Konten, gefälschten Dokumenten und Malware zu entdecken. Dies hilft bei der Identifizierung von Tätern und der Verhinderung weiterer Schäden. Ein besonders wichtiger Aspekt ist die Informationsgewinnung: Das Darknet kann wertvolle Informationen über neue Angriffsmethoden, Exploits und Schwachstellen liefern. Durch die Analyse dieser Informationen können Sicherheitslücken geschlossen und präventive Maßnahmen ergriffen werden. Durch das Monitoring können auch Schwachstellen-Börsen in Darknet gefunden werden, die Hinweise auf neue Angriffsformen aufzeigen.

Effektives Darknet-Monitoring

Es gibt eine Vielzahl von Produkten, die speziell für das Darknet-Monitoring und die -Analyse entwickelt wurden. Diese umfassen Suchmaschinen, Forenüberwachung, Datenbankabfragen und Künstliche Intelligenz, um verdächtige Aktivitäten zu erkennen und zu verfolgen. So wie das Cyber Crime sich immer weiter vernetzt, sollten sich viele Firmen, gerade auch kleinere, nicht davor scheuen, die Chance zu nutzen und mit den Behörden in Kontakt zu treten. Dabei ist die Zusammenarbeit mit Strafverfolgungsbehörden entscheidend, um Informationen auszutauschen, Ermittlungen durchzuführen und Täter zu identifizieren. Oft bietet sich auch der Verfassungsschutz als ideale Plattform für Unternehmen, da dieser, im Gegensatz zu Strafverfolgungsbehörden, nicht gleich ermitteln muss.

SOC Service als Ideallösung

SOC – Security Operation Center – eine Art digitaler Werkschutz – ist das Zauberwort und die Lösung für jede Firma. Hochspezialisierte Mitarbeiter und Technologien werden hier zusammengeführt, um gerade auch Darknet-Monitoring und -Analysen durchzuführen. Firmen, die diesen Aufwand nicht leisten können, haben heute die Chance, bei einem der vielen Anbietern von „SOC-Service“ sich die passenden Dienste einzukaufen. Auch für größere Unternehmen ist es oft leichter, durch den Zukauf solcher Leistungen die eigene IT-Security abzurunden. Denn ein erfolgreicher Angriff kann das Vielfache solcher Dienstleistungen kosten.

„Durch das Überwachen des Darknets können Sicherheitsbehörden und Unternehmen frühzeitig potenzielle Bedrohungen erkennen.“

Boris Bärmichl,
Vorstandsmitglied des BVSW e.V.

Live-Webcast des BVSW zu „ChatGPT“

Die Betreiber von ChatGPT sehen die positiven Aspekte, denn eine neue, schnelle und hoch automatisierte Welt entsteht. „Reich werden, ohne zu arbeiten“ – das ist ihre Parole. Oder ist es doch nur der Ausverkauf von allem, was im Internet zu finden ist? Wird Copyright bald der Geschichte angehören? Dieser Webcast zeigt beide Seiten. Die Teilnehmer werden „Live“ auf die verschiedensten KI-Plattformen gehen und sich selbst ein Bild machen.
Die Veranstaltung findet via MS Teams am 14.6.2023 von 14 bis 16 Uhr statt.
Referent: Boris Bärmichl

Anmeldungen unter:
www.bvsw.de/aus-und-weiterbildung

Doch wie finde ich den richtigen Service Partner, woran erkenne ich, ob dieser sein Geschäft beherrscht? Es gibt ein paar wesentliche Aspekte. Zunächst einmal: Ein idealer Partner ist 24/7 für den Kunden da; es handelt sich dabei nicht um ein Call Center, sondern einen 24h-Schichtbetrieb mit deutschsprachigem Personal. Warum ist das so wichtig? In der Krise braucht man die direkte Kommunikation in der Muttersprache. Moderne SOCs setzen auf Technologien wie XDR, EDR und NDR-Technologien, um Angreifer auszusperren oder einzudämmen. Wenn man das Unternehmen unter den qualifizierten APT Response Dienstleistern des Bundesamtes für Sicherheit in der Informationstechnik findet, ist das ein weiteres Qualitätsmerkmal. Zudem sollte der SOC-Service-Anbieter mindesten 45 IT-Security Spezialisten und Festangestellt haben. Wenn alle diese Punkte zutreffen, sollte man die Preise und Leistungen vergleichen und auch darauf achten, dass die Datenschutz-Grundverordnung eingehalten und nachgewiesen werden kann. Sollte das alles nicht weiterhelfen, kann man auch Kontakt zum BVSW e.V. aufnehmen, der gerne weiterhilft. ■