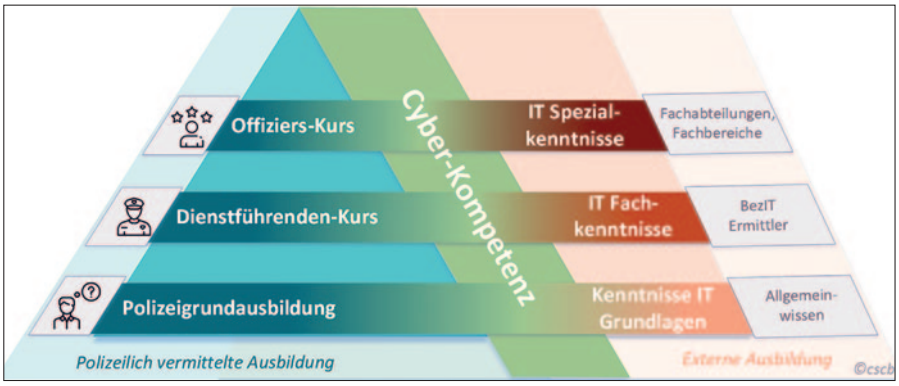
Cyber-Kompetenzen fördern

Aufgrund der fortschreitenden Digitalisierung ist es wesentlich, dass die Mitarbeiterinnen und Mitarbeiter einer Sicherheitsbehörde über die notwendigen Kompetenzen im Umgang mit der Technik und im Verhalten mit Cyber-Bedrohungen verfügen.

Themen wie Risiko-Management und Digitalisierung haben im Bundesministerium für Inneres (BMI) schon in vielen Bereichen Fuß gefasst. Doch wie sieht es mit den Cyber-Kompetenzen aus? Cyber-Bedrohungen sind zu einer allgegenwärtigen Herausforderung geworden. Sie gefährden nicht nur die Sicherheit unserer Daten und Systeme (und damit auch Menschen), sondern auch das Vertrauen, das wir in die digitale Infrastruktur setzen. Um gegen diese Bedrohungen gewappnet zu sein, ist es wichtig, in den Organisationen eine hohe Cyber-Kompetenz aufbauen. Als Sicherheitsbehörde ist es entscheidend, dass sich das BMI mit dem Stand der Technik mitentwickelt und Cyber-Kompetenz unter seinen Bediensteten fördert.

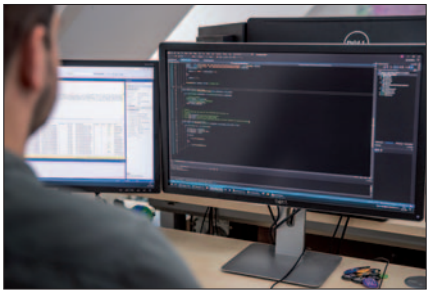
Cyber-Kompetenz ist für die Bediensteten einer Sicherheitsbehörde notwendig für das Verständnis bei der Entwicklung, Problemen sowie Möglichkeiten und Grenzen der Digitalisierung – in Bezug auf Cyber-Sicherheit und die Bekämpfung von Cyber-Kriminalität. Sie ermöglicht es, operative und strategische Entscheidungen bei digitalen Ermittlungen und in der digitalen Forensik zu treffen, die kurz- und langfristige Auswirkungen auf den Betrieb von polizeilichen und kriminalpolizeilichen Dienststellen haben. Dazu gehört zumindest ein Einblick in Materien wie Cyber-Kriminalität, Cyber-Sicherheit, Cyber-Prävention, digitale Forensik, Stakeholder in Wirtschaft und Wissenschaft und kompetente Ansprechpartner und Experteninnen und Experten.

Status quo der Cyber-Kompetenz im BMI. Die klassische Polizeiarbeit hat sich durch die Digitalisierung in den letzten 20 Jahren maßgeblich verändert. Cybercrime ist nur ein Teilbereich des neuen Aufgabengebietes digitaler Polizeiarbeit und hat durch enorme Steigerungsraten seit Beginn der statistischen Aufzeichnungen von sich reden gemacht. Aber gerade im Bereich der Strafverfolgung und Beweismittelsicherung hat der „digitale Tatort" einige Überraschungen mit sich gebracht. Die digitale Forensik spielt eine immer größer werdende Rolle. Waren in den Anfangszeiten der Beweismittelsicherung überwiegend kinderpornografische Inhalte im Fokus der IT-Ermittler und IT-Forensiker – so hat sich das Blatt mittlerweile gewendet. Jeder Täter, jedes Opfer und jeder Zeuge hat Datenträger, die entweder sichergestellt oder als Beweismittel beigebracht, gesichert und aufbereitet werden müssen. Und hier werden die immer größer werdenden Datenmengen schlagend.



Umsetzung von Cyber-Kompetenzen in bestehenden Organisationsstrukturen

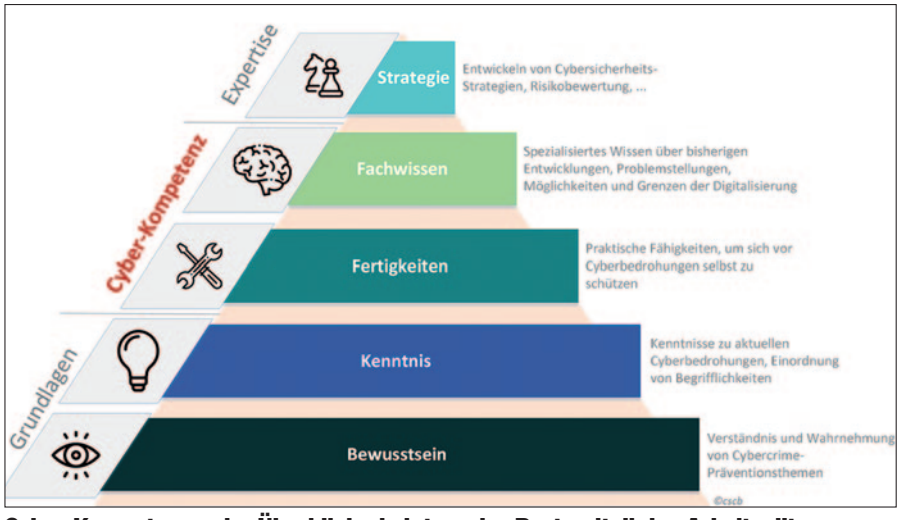
Hatte in den Anfangszeiten der digitalen Beweismittelsicherung eine Festplatte vielleicht 40 Gigabyte mit z. B. 20.000 Bildern – können es heute Datenträger mit mehreren Terabyte sein und 1 Million an Bildern enthalten. Dies führt zu einem höheren Bearbeitungs- und Zeitaufwand bei der Sicherung und Sichtung der Inhalte, bindet Personal und erfordert teure und leistungsfähige IT-Systeme und Software. Es leistet forensische Soft- und Hardware immer mehr in diesem Bereich – dies erfordert jedoch ein immer größer werdendes technische Know-how. Neben der Technik müssen sich die BMI-Bediensteten mitentwickeln. Dabei zählen nicht nur technische Fähigkeiten und Fertigkeiten – es muss nicht jeder IT-Profi werden –, sondern es kommt vielmehr auf das Bewusstsein für Bedrohungen und Risiken an. Es muss eine Sicherheitskultur in der Organisation und in der digitalen Arbeitswelt entwickelt und die Verhaltensweisen müssen angepasst werden. Eine solche Anpassung muss bei den Führungskräften beginnen. Man könnte dies auch als eine Erzeugung „interner Awareness" bezeichnen, die erforderlich ist – um einen digitalen Weitblick zu ermöglichen.



Cyber-Kompetenzen sind essenziell für eine erfolgreiche Bekämpfung von Kriminalität und digitale Polizeiarbeit

Um Cyber-Kompetenz auch im BMI zu etablieren, werden neue Wege erforderlich sein. Die Anstellung von Quereinsteigern, Cyber-Recruiting in den eigenen Reihen, spezielle Aus- und Fortbildungen sind dabei einige Möglichkeiten. Fachkräftemangel gibt es überall und IT-Spezialistinnen und -spezialisten zu finden, zu rekrutieren, zu motivieren und zu „pflegen" ist eine Herausforderung, da man dieses Know-how nicht über Nacht „erzeugen" kann. Cyber-Kompetenz ist essenziell für eine erfolgreiche Bekämpfung von Kriminalität und Funktion digitaler Polizeiarbeit. Besonders wichtig ist es, für das interne Bewusstsein zu

Foto: Gerd Pachauer, Grafik: CSCB



Cyber-Kompetenzen im Überblick als integraler Bestandteil des Arbeitsalltags

sorgen und Cyber-Kompetenz Führungskräften zu vermitteln. Nur wer über eine geeignete Cyber-Kompetenz verfügt, kann operative und strategische Entscheidungen im Cyber-Bereich treffen. Beschaffung, Personalwerbung, Cyber-Projekte, Aus- und Fortbildung sind nur dann funktionell und effizient, wenn fachlich fundierte Cyber-Entscheidungen getroffen werden.

Ein Beispiel: 24/7 – Cyber-Kompetenz durch einen Landes-IT-Dienst. In Kärnten wird seit rund einem Jahr vom Landeskriminalamt als Pilotprojekt und sehr erfolgreich ein Landes-IT-Dienst bereitgestellt. Dieser Landes-IT-Dienst ist 24/7 verfügbar und unterstützt Kolleginnen und Kollegen telefonisch oder persönlich in allen Fragen zum Thema Cybercrime im engeren Sinn sowie bei Erstmaßnahmen im Zuge einer unvorhersehbar eintretenden Sicherstellung von Daten und Datenträgern, wenn z. B. der zuständige Bezirks-IT-Ermittler nicht erreichbar ist. Der Landes-IT-Dienst wird von Mitarbeitern des AB 06 IT-B (Informationstechnologie/Beweissicherung) und Bezirks-IT-Ermittlern gemeinsam betrieben und deckt in erster Linie alle technisch erforderlichen Erstmaßnahmen und Problemstellungen ab, um eine forensisch korrekte Vorgehensweise sicherzustellen. Bereits im ersten Jahr wurde dabei rund 450 Serviceleistungen für Dienststellen und Kolleginnen und Kollegen in Kärnten erbracht.

Cyber-Kompetenz „by Design“. Im Bereich von IoT (Internet der Dinge) ist Security by Design – also Sicherheit ab Werk – z. B. in Smart-Home-Geräten schon lange relevant für IT-Sicherheit. Cyber-Kompetenz by Design schlägt dabei in die gleiche Kerbe. Um eine gute Basis für Cyber-Kompetenz vor allem in der IT-Ermittlung oder IT-Forensik zu schaffen, ist es erforderlich, bereits bei der Personalsuche auf einschlägige Schulbildung oder Fachkenntnisse zu reflektieren. HTL-Absolventen, FH- und Universitätsabschlüsse mit technischem Background stellen ebenso wie einschlägige Fortbildungen in der Netzwerktechnik, IT-Security etc. eine Möglichkeit dar, schneller ein entsprechendes Qualitätsniveau zu erreichen. Es sollten bewusst jene Personen angesprochen werden, die über entsprechende Fachkenntnisse verfügen. Dieser Prozess sollte dabei so früh wie möglich erfolgen, um geeignete Fachkräfte für eine Verwendung im Cyber-Bereich der Polizei zu gewinnen. In Kärnten wird diese spezielle Art der Interessentensuche bereits seit rund einem Jahr in Zusammenarbeit mit dem Bildungszentrum in Krumpendorf erfolgreich betrieben und sorgt für steten Nachwuchs bei der Bezirks-IT-Ermittlung.

Cyber-Kompetenz als Führungsaufgabe. Aber auch bei Führungskräften im BMI ist während der Ausbildung sowie bei ihrer Tätigkeit darauf zu achten, dass die Cyber-Kompetenz immer wichtiger wird. Führungskräfte treffen oft Entscheidungen, die erhebliche Auswirkungen auf die Sicherheit und das Risikomanagement einer Organisation haben können. Sie müssen daher in der Lage sein, Risiken und Auswirkungen von Cyber-Bedrohungen zu verstehen, um fundierte Entscheidungen zu treffen und angemessene Schutzmaßnahmen zu ergreifen. Zudem spielen sie eine wichtige Rolle bei der Schaffung und Förderung einer Sicherheitskultur in einer Organisation. Sie können beispielsweise durch ihre Handlungen und Einstellungen ein Vorbild für Mitarbeiter sein und damit zur allgemeinen Cyber-Kompetenz in der Organisation beitragen. Darüber hinaus ist Cyber-Kompetenz für Führungskräfte wichtig, um effektiv mit technischen Bereichen, die aufgrund der fortschreitenden Digitalisierung immer häufiger beigezogen werden, kommunizieren zu können. Sie müssen in der Lage sein, technische Grundlagen und Risikobewertungen zu verstehen und diese Informationen in strategische und operationelle Entscheidungen umzusetzen. Schließlich sind Führungskräfte auch oft das Ziel von Cyber-Bedrohungen, bei denen Cyber-Kriminelle versuchen, vertrauliche Informationen zu erhalten.

Schlussfolgerungen. Cyber-Kompetenz ist nicht nur eine Angelegenheit des IT-Teams, sondern eine Aufgabe für die gesamte Organisation. Jeder Mitarbeiter, jede Mitarbeiterin trägt zur Cyber-Sicherheit bei und muss regelmäßig geschult werden. Die Etablierung einer starken Cyber-Kompetenz erfordert eine Kultur des kontinuierlichen Lernens und der ständigen Verbesserung. Organisationen müssen Wege finden, um dieses Lernen zu fördern und zu unterstützen. Praktische und theoretische Schulungen, Zertifizierungen, Simulationsübungen und Awareness-Kampagnen können wirksame Instrumente zur Steigerung der Cyber-Kompetenz darstellen. Die Anpassung von Strategien an die spezifischen Bedürfnisse und Herausforderung des BMI ist entscheidend für die zukünftige Weiterentwicklung. Darüber hinaus ist es erforderlich für spezielle Bereiche ein besonderes Cyber-Recruiting zu betreiben. Ebenso wichtig ist es auch, in eigene Expertinnen und Experten zu investieren und Vertrauen in ihre Fähigkeiten zu setzen, die über viele Jahre hinweg kostbares Wissen und Erfahrungen aufgebaut haben. Viele von ihnen haben das Gros ihrer Kenntnisse auf eigene Kosten und in ihrer Freizeit über Jahre hinweg aufgebaut und stellen dies der Organisation zur Verfügung.

Christian Baumgartner
Christina Schindlauer

GRAFIK: CSCB