Titel der Rede	Resilienz im Cyberraum: Die Cybersicherheit im Lichte der aktuellen Bedrohungslage, Cybercrime und KI
Datum/ Zeit/ Ort	12. Juni 2024, 09:30 Uhr, Hotel Adlon Berlin, Hauptsaal
Redezeit	15_ Minuten (+ 5 Minuten Q&A)
Kontakt zum Veranstalter	
Beschreibung der Veranstaltung/ Redesituation/ Anlass	• Fachkongress Deutschland für IT- und Cybersicherheit bei Staat und Verwaltung • Setting: stehend, Pult, bis 30 Min vor Beginn die Wahl zwischen Mirco oder Verkabelung (beim Moderator melden)
Publikum	

PITS Keynote für Frau Dahns am 12. Juni 2024

Es gilt das gesprochene Wort.

Sehr geehrte Damen und Herren,

ich freue mich sehr, Ihnen im Rahmen dieser Keynote einen Einblick in unsere Arbeit und Aufstellung hinsichtlich der Resilienz im Cyberraum zu geben.

Herzliche Grüße von Frau Dahns, deren Präsenz zeitgleich im Innenausschuss des Deutschen Bundestages zu einem aktuellen Thema erbeten ist.

Ich darf Frau Dahns kurzfristig vertreten. Mein Name ist Daniel Meltzian und ich leite das Grundsatzreferat Cyber- und Informationssicherheit im BMI.

Wir befassen uns in der Abteilung CI mit einer ganz bunten und vielfältigen Mischung an Themen: Diese reichen von der Fortentwicklung der Cybersicherheitsarchitektur über internationale Cybersicherheit und Cybersicherheitsforschung bis zur Cybersicherheit in der Wirtschaft und der Bundesverwaltung. Weiter gehören dazu die Gewährleistung der Netzinfrastruktur der öffentlichen Verwaltung/des Digitalfunks und der Cyberfähigkeit der Sicherheitsbehörden, rechtlich, technisch und lagebezogen!

Die Europameisterschaft und weitere anstehende Großereignisse machen angesichts der aktuellen Cybersicherheitslage die Notwendigkeit einer erhöhten Resilienz im Cyberraum und unsere Bemühungen im Bereich der Cybersicherheit deutlich. Ein besonderes Anliegen war Frau Dahns daher in den ersten beiden Monaten im neuen Amt auf alle Partner zuzugehen, die bei derartigen Großereignissen dazu beitragen die (Cyber-)sicherheit zu gewährleisten.

Das BMI betrachtet die Cybersicherheit nach dem Leitbild des BSI im Dreiklang Prävention, Detektion und Reaktion:

Prävention zum Beispiel durch Zertifizierung und Beratung des BSI, Detektion als Meldestelle und Reaktion in der Gestalt von konkreten Anordnungen und Eingriffen insbesondere auch zur Zerschlagung schädlich genutzter Infrastruktur.

Von der Wirtschaft, über das politische und gesellschaftliche Miteinander, vom Beruf bis hin zum privaten Umfeld - In einer so umfänglich vernetzten Welt wie der heutigen, betrifft **Cyberresilienz alle Lebensbereiche**.

Gleichzeitig zeigen uns jedoch sowohl der BSI-Lagebericht des vergangenen Jahres, als auch das vor Kurzem veröffentliche

Bundeslagebild Cybercrime, dass die Bedrohungslage im Cyberraum für Deutschland so hoch wie noch nie ist und die Bedeutung von Cyberresilienz nicht unterschätzt werden sollte.

Ein **paar Daten** für Sie:

- Das BSI hat im Berichtszeitraum 2023, also innerhalb eines Jahres, täglich **rund 250.000 neue Varianten von Schadprogrammen** und **21.000 mit Schadsoftware infizierte Systeme** registriert.
- Hinzu kommen **durchschnittlich 70 neue Sicherheitslücken** pro Tag. Jede zweite davon wird als hoch bedeutsam oder kritisch eingestuft. Das entspricht einer Steigerung von 24 Prozent

gegenüber dem Vorjahr. Cybercrime. Vor allem Ransomware, stellt hierbei die größte Bedrohung dar.

Unsere globale Vernetzung und die fortschreitende Digitalisierung vergrößern zudem die Angriffsfläche: Es sind mehr Dienstleistungen online und zunehmend vernetzt, so dass aufgrund von Abhängigkeiten bei Lieferketten oder bei vernetzten Systemen ein Angriff auf das schwächste Glied große Folgen haben kann.

Umso wichtiger ist, dass wir dem entgegentreten, uns besser schützen und unsere **Cyberresilienz stärken**:

Um Resilienz zu stärken und dem Präventionsgedanken im Sinne unseres Dreiklangs zu entsprechen, ist es unerlässlich, bei dem Fundament zu anzusetzen; das heißt die **gesetzlichen Rahmenbedingungen** anzupassen.

Eine dieser Rahmenbedingungen ist das **NIS2 Umsetzungs- und Cybersicherheitsstärkungsgesetz**.

Wie Sie wissen, arbeitet das Bundesinnenministerium zurzeit an einer **umfassenden Reform** des deutschen IT-Sicherheitsrechts.

Mit der Umsetzung der NIS-2-Richtlinie werden in der gesamten EU zukünftig mehr Unternehmen in insgesamt mehr Sektoren wie Energie, Verkehr, Gesundheit und digitale Infrastruktur **Cybersicherheitsvorgaben** sowie Meldepflichten bei Cybervorfällen erfüllen müssen. Dabei ist von besonderer Bedeutung, dass das Gesetz den bisherigen Kreis der betroffenen Unternehmen erheblich ausweitet.

So steigern wir das Sicherheitsniveau – und senken damit das Risiko für Unternehmen und Verwaltung, Opfer von Cyberangriffen zu werden.

Ich bin davon überzeugt, dass es uns zudem gelingen wird, mit dem Gesetz die Resilienz von Wirtschaft und Bundesverwaltung gegenüber Cybergefahren zu stärken.

Zum ersten Mal wird mit der NIS-2-Richtlinie auch die öffentliche Verwaltung mit drei Ebenen erfasst. Die ersten beiden Ebenen, in Deutschland die Bundes- und Länderebene, sind verpflichtend vorgegeben. Die Aufnahme der dritte Ebene, die Kommunalebene, liegt nach der Richtlinie im Ermessen des Mitgliedstaats und innerstaatlich in der Kompetenz der Länder.

Sie sehen also, der Umsetzungsaufwand aber auch die Notwendigkeit dieser Schutzmechanismen in Deutschland ist beachtlich!

Ich möchte nun auf den Phänomenbereich „Cybercrime“ und das BKA Bezug nehmen.

Cyberkriminalität zählt mittlerweile zu den allgegenwärtigen Bedrohungen, so das jüngste, am 13. Mai 2024 veröffentlichte, **Bundeslagebild Cybercrime 2023**: Es gehört bereits seit Jahren zu den kriminalpolizeilichen Phänomenbereichen mit dem höchsten

Schadenspotenzial in Deutschland - nach Erhebungen des Branchenverbandes Bitkom e.V. lagen für das Jahr 2023 die durch Cyber-Angriffe verursachten gesamtwirtschaftlichen Schäden bei 148 Milliarden Euro.

Kriminelle Dienstleistungen werden hierbei im Geschäftsmodell **„Crime-as-a-Service“** von Tätergruppierungen angeboten, die weitgehend anonym und dezentral zusammenarbeiten. Neben finanzstarken Unternehmen standen Einrichtungen und Institutionen mit hoher Öffentlichkeitswirksamkeit im Fokus. Es waren aber auch leicht verwundbare kleine und mittelständische Unternehmen stark betroffen.

2023 war auch geprägt von **hacktivistischen DDoS- Kampagnen** und einer Vielzahl an **Ransomware-Angriffen** – letztere stellen bereits seit mehreren Jahren die Top-Bedrohung im Bereich Cybercrime dar.

Eine Auswertung des BKA und der Landeskriminalämter zeigt: Im Jahr 2023 haben bundesweit über **800 Unternehmen** und Institutionen Ransomware-Fälle bei der Polizei zur Anzeige gebracht; von einer hohen Dunkelziffer [geschätzt 90%] ist auszugehen. Im vergangenen Jahr überstiegen zudem die weltweiten Lösegeld-Zahlungen bei Ransomware erstmalig die Marke von 1 Milliarden US-Dollar.

Auch dieser Überblick zeigt die steigende Gefährdungslage im Cyberraum. Besonders eingehen möchte ich auch auf die Ermittlungserfolge des BKA in diesem Bereich, welche wiederum abschließen den dritten Teil unseres Dreiklangs „Reaktion repräsentieren. Diesen problematischen Entwicklungen stehen auch bemerkenswerte Ermittlungserfolge des Bundeskriminalamts zusammen mit deutschen und internationalen Polizeibehörden in den vergangenen Monaten gegenüber, welche die internationale cyberkriminelle Szene geschwächt haben. Als Beispiele möchte ich hier die Abschaltung der Krypto-Geldwäscheplattform „ChipMixer“, die Beschlagnahme des kriminellen Darknet-Marktplatzes „Genesis Market und - erst jüngst, vor

knapp 2 Wochen - den Takedown einer ganzen Reihe gefährlicher Schadsoftwarefamilien und ihrer kriminellen Infrastrukturen im Rahmen der internationalen Operation „Endgame““ nennen. Diese Operation, bei der unter Federführung der Generalstaatsanwaltschaft Frankfurt am Main und des Bundeskriminalamts zusammen mit internationalen Partnern über 1500 kriminell genutzte Server und Domains unschädlich gemacht, Krypto-Geldwerte mit einem aktuellen Gesamtvolumen in Höhe von mehr als 70 Millionen Euro bei Kryptobörsen gesperrt und allein von Deutschland acht Haftbefehle erlassen wurden, kann als der bislang größte Schlag gegen die weltweite Cyberkriminalität angesehen werden. Die Ermittlungserfolge zeigen einmal mehr, dass sich Straftäter auch im

Internet nicht dem Zugriff durch die Strafverfolgungsbehörden entziehen können.

Ein nicht zuletzt vielseitiges und beachtenswertes Themenfeld ist die Künstliche Intelligenz.

Das BMI ist Antreiber für verantwortungsvolle KI!

Das BMI ist Entwickler, Auftraggeber und Nutzer von KI-Anwendungen. Die Bundesverwaltung kann wesentlich dazu beitragen, den KI-Standort Deutschland zu stärken und Vertrauen und Akzeptanz in KI zu erhöhen.

Wir möchte das immense Potenzial von KI nutzen und zugleich hohe Standards setzen: für die digitale Souveränität der Bürgerinnen und Bürger, die IT-Sicherheit und den Schutz persönlicher Daten.

Dabei ist es für uns wichtig, bestehende Initiativen miteinander enger zu vernetzen, auf diesen Strukturen aufzubauen und Doppelstrukturen zu vermeiden. Daneben werden wir mit z.B. dem Beratungszentrum Künstliche Intelligenz (BeKI) auch den KI-Kompetenzaufbau in der Bundesverwaltung in der Breite unterstützen, um hierdurch die Akzeptanz in die Technologie zu stärken.

Weiterhin investieren wir in die Forschung zu KI. Namentlich ist dabei die BSI-Studie „Auswirkungen von KI auf die Cyberbedrohungslandschaft“ zu nennen, welche Cyberangriffe und die Verteidigungsmöglichkeiten beschreibt, die sich durch den Einsatz von KI, insbesondere Large Language Modells ergeben bzw. ergeben können.

Wichtig ist hierbei, dass die KI für Sicherheitsbehörden einsetzbar sein muss.

Es bestehen große Herausforderungen für den aktuellen und zukünftigen Einsatz von KI bei Sicherheitsbehörden. Der Einsatz von KI kann die Effizienz der Arbeit von Sicherheitsbehörden erhöhen und stellt die Handlungsfähigkeit der Sicherheitsbehörden gegenüber potentiell

feindlichen Akteuren sicher, welche KI zum Schaden von Gesellschaft und Sicherheit einsetzen wollen.

Die Gesellschaft und Politik haben höchste Erwartungen an den Einsatz von KI bei Sicherheitsbehörden: Sie muss vertrauenswürdig sein und verantwortungsvoll eingesetzt werden.

Angesichts der sich verändernden Bedrohungslandschaft ist es wichtig, der Cybersicherheit höchste Priorität einzuräumen. Es wird entscheidend sein, die Geschwindigkeit und den Umfang der Abwehrmaßnahmen zu erhöhen.

Wir haben die Risiken von KI für unsere Demokratie und unsere Sicherheit fest im Blick und treten Desinformation entgegen.

Die gezielte Verbreitung von falscher oder irreführender Information, sogenannter Desinformation, stellt eine zunehmende Bedrohung für die innere Sicherheit, den gesellschaftlichen Zusammenhalt und die freiheitliche demokratische Grundordnung in Deutschland dar.

Deepfakes, die Stimmen oder Gesichter imitieren oder verfälschen, können hier ein sehr gefährliches Mittel sein. Gleiches gilt für das künstliche Verstärken demokratiefeindlicher Narrative.

Wir brauchen auch gesetzliche Antworten wie klare Kennzeichnungspflichten. Mindestens genauso wichtig ist die Aufklärung und Sensibilisierung unserer Gesellschaft.

Das BMI sensibilisiert die Bürgerinnen und Bürger vor den Gefahren von Desinformation als illegitime Einflussnahme sowie vor sog. Deepfakes, u.a. auf seiner Website. Sowohl international (u.a. EU, G7, NATO) als

auch national steht das BMI in Kontakt mit der Zivilgesellschaft und den Ländern zum Thema Desinformation.
In den nächsten Wochen haben wir mit der Fußball EM im eigenen Land und den Olympischen Spielen im Nachbarland Frankreich Großereignisse mit besonderer Strahlkraft. In diesen Wochen werden wir zeigen, dass wir gut vorbereitet sind und – um im Fußball Bild zu bleiben - wie stark die Abwehr in der Cybersicherheit steht. Vielen Dank für Ihre Aufmerksamkeit!