Prof. Jan S. Hesthaven, Präsident des Karlsruher Instituts für Technologie

27. November 2025

Keynote beim Cyber Security Forum 2025

Meine Damen und Herren,
vielen Dank, dass Sie sich die Zeit genommen haben, heute Morgen hier zu sein. Ich möchte auch den Organisatorinnen und Organisatoren dieser spannenden Veranstaltung für die Einladung danken, hier zu sprechen und einige persönliche Perspektiven aus meiner Rolle als Präsident des Karlsruher Institut für Technologie einzubringen.

Ich möchte einige allgemeine Herausforderungen für Universitäten diskutieren, die sich aus den sehr dynamischen Zeiten ergeben, in denen wir leben. Diese Dynamik erzeugt Spannungsfelder, die teils im Widerspruch zu den Grundprinzipien einer traditionellen Universität stehen. Wie ich gleich erläutern werde, entstehen daraus anspruchsvolle Situationen – politisch, gesellschaftlich und ganz besonders im Bereich der digitalen Sicherheit.

Die traditionelle Universität zeichnet sich durch offene, vertrauensbasierte und international vernetzte Gemeinschaften aus, in denen Informationen, Daten und Wissen frei ausgetauscht werden, um Erkenntnisse zu gewinnen. Dieser Austausch findet in der Regel in kleinen Gemeinschaften internationaler Kooperationspartner statt, oft ohne klare Grenzen, wer was mit wem teilen darf.

Darüber hinaus werden Universitäten traditionell als Konföderationen mit stark autonomen Einheiten geführt. Am KIT sind dies 415 einzelne Gruppen – die Professuren – mit einer ausgeprägten Selbstständigkeit, über die die zentrale Organisation vor allem Soft Power hat und nur sehr begrenzte Hard Power ausüben kann.

Für einige von Ihnen aus der Wirtschaft mag dies wie eine herausfordernde Konstellation erscheinen – und das ist sie auch. Stellen Sie sich Deutschland nicht mit 16 Bundesländern vor, sondern mit 415 – bei noch schwächerer zentraler Steuerung.
Gleichzeitig ist dies ein Modell, das seit der Gründung der ersten Universitäten vor rund 800 Jahren im Wesentlichen stabil geblieben ist. Kaum eine andere westliche Institution hat eine vergleichbare Tradition – außer der katholischen Kirche.

Diese Struktur – sowohl in ihrer Arbeitsweise als auch in ihrer Führung – steht heute unter erheblichem Druck. Lassen Sie mich einige der Herausforderungen nennen, die mich zugegebenermaßen gelegentlich nachts wach liegen lassen.

Geopolitik: Die zunehmende Polarisierung stellt unsere traditionelle Ausrichtung auf Leistung und wissenschaftliche Qualität vor Nationalität in Frage. Wissenschaft lebt vom offenen Austausch, doch gerade dieser wird politisch schwieriger. Für Organisationen, die sich der Diplomatie durch Wissenschaft verpflichtet fühlen, bedeutet dies eine historische Umstellung.

Demografie: Das Durchschnittsalter in Deutschland liegt bei über 48 Jahren – weltweit fast Spitzenwert und wird lediglich von Japan übertroffen. Ähnliche Trends sehen wir in Europa und Asien, während Länder wie die USA oder Indien besser dastehen. Für Universitäten bedeutet dies: weniger junge Menschen, weniger Bewerber, mehr Konkurrenz – und für die Wirtschaft massive Fachkräfteengpässe. Die klassische Antwort lautet internationale Rekrutierung – aber: Wo sind die jungen Menschen? Vor allem in Subsahara-Afrika und auf der Arabischen Halbinsel. Doch dort sind gesellschaftliche Unterstützung, Integrationsmöglichkeiten und Vorbildungsniveaus oft heterogener, was die Hochschulen vor neue Herausforderungen stellt.

Politischer Aktivismus: Universitäten werden zunehmend aufgefordert, Haltung zu politischen Fragen einzunehmen – zur Flüchtlingspolitik, zu extremistischen Tendenzen, zum Gaza-Konflikt oder aktuell zur sicherheits- und verteidigungsbezogenen Forschung. Dies verändert unsere Rolle als traditionell politisch neutrale, diskursorientierte Institutionen.

Vielfalt: Mehr Internationalität bedeutet: mehrsprachige Angebote, kulturelle Sensibilisierung, neue Unterstützungsstrukturen. Gleichzeitig steigt der Anteil neurodivergenter Studierender – eine Chance, aber auch eine Herausforderung, da Lern- und Prüfungsformate angepasst werden müssen. Beide Gruppen sind in den letzten zehn Jahren stark gewachsen.

KI: Und schließlich das rasante Aufkommen der KI in Bildung, Forschung und Verwaltung. Die Herausforderung liegt nicht in der KI selbst, sondern in der Geschwindigkeit, mit der wir uns anpassen müssen. Eine deutsche Institution mit 800 Jahren Tradition ist vieles, aber nicht schnell.
Ein Beispiel: Die Einrichtung eines neuen Studiengangs dauert meist drei Jahre – vor drei Jahren existierte die heutige KI-Landschaft noch nicht. Wenn wir uns nicht rasch anpassen, besteht die Gefahr, als Institution an Relevanz zu verlieren.

Was hat das alles mit Cybersicherheit zu tun?

Für Universitäten – offen, vertrauensbasiert, dezentral und mit der Tradition des „Bring your own device“ – bedeutet es, dass wir besonders verwundbar sind. Und tatsächlich waren Universitäten in den letzten zehn Jahren zunehmend Ziel von Cyberangriffen.

2021 wurden 26 US-amerikanische Einrichtungen von Ransomware angegriffen – doppelt so viele wie im Jahr zuvor.
Das Technion in Israel wurde von einem staatlich unterstützen Akteur angegriffen und musste seine IT-Systeme drei Monate lang komplett herunterfahren.
Ein ähnlicher Vorfall traf ein Fraunhofer-Institut.

Im November dieses Jahres wurde die University of Pennsylvania Opfer eines Angriffs mit einer massiven Datenpanne: 1,2 Millionen Dateien mit personenbezogenen Daten und sogar geschätzten Vermögenswerten (!) von Studierenden, Alumni und Spendern wurden erbeutet.

Die Ziele solcher Angriffe sind vielfältig – Lösegeldforderungen, Datendiebstahl, wissenschaftliche Spionage oder politisch motivierte Sabotage.

Die meisten Angriffe beginnen mit Phishing oder CEO-Fraud, gefolgt von komplexeren Techniken, sobald die erste Verteidigungslinie durchbrochen ist. Das wird erleichtert durch offene Netzwerkphilosophien, veraltete Systeme oder Geräte, die aus wissenschaftlichen Gründen nicht aktualisiert werden können – am KIT laufen einzelne Spezialinstrumente tatsächlich noch auf Windows 95.

Wie sieht die Lage am KIT aus?

Eine Organisation mit 10.000 Mitarbeitenden, 23.000 Studierenden, Hunderten von Gästen jährlich, verteilt auf 6 Standorte – und mit 415 autonomen Professuren, die oft auch in Fragen der IT-Sicherheit eigene Wege gehen.

Wir hosten rund 12.000 Domainnamen und betreiben 2.200 virtuelle Desktops auf 100 Hosts.
Unsere Sicherheitsarchitektur besteht aus mehreren Ebenen: Eine erste Firewall mit hoher Offenheit dahinter, sowie vier zusätzliche Zonen, um besonders sensible Daten in einer No-Trust-Umgebung zu schützen.
Hinzu kommen 6.000 Netzwerksegmentierungen, viele davon lokal verwaltet.

Unser CERT-KIT – eines der ältesten an deutschen Universitäten – und die zentrale IT-Sicherheitsorganisation leisten großartige Arbeit. Sie haben das KIT bislang vor größeren Schäden bewahrt.

Aber die Lage verschärft sich: Die Angriffe haben sich in den letzten Jahren jährlich verdoppelt.
Bis zu 85 % der E-Mails an KIT-Adressen werden aussortiert.
KI-generierte Angriffe machen die Erkennung immer schwieriger.
Es ist realistisch anzunehmen, dass die Frage nicht lautet *ob*, sondern *wann* ein größerer Vorfall eintritt.

Was tun wir? Wir informieren, sensibilisieren, priorisieren, schützen sensible Daten.
Doch: Die Durchsetzung zentraler Vorgaben stößt schnell an die Grenzen universitärer Kultur – Autonomie, Offenheit, lokale Eigenverantwortung.
Genau hier liegt der Kern der Herausforderung.

Können wir mehr tun? Sicher. Aber IT-Sicherheit ist für Universitäten a) neu, b) teuer und c) intern nicht immer beliebt. Stärkere zentrale Eingriffe wären schwer durchsetzbar.

Was etwas beruhigt: Universitäten sind wichtige, aber keine systemkritischen Einrichtungen. Eine vorübergehende Schließung hat unangenehme, aber keine existenziellen Folgen. Und: Wir verdienen kein Geld, wir geben es aus – das macht uns für klassische Ransomware weniger attraktiv.

Zusammenfassend:
Unsere Welt hat sich in den letzten zehn Jahren so entwickelt, dass traditionelle

Werte der Universitäten – Offenheit, Vertrauen, lokale Governance, begrenzte zentrale Kontrolle, Vielfalt – zunehmend unter Druck geraten.

Dies betrifft nicht nur unsere Organisation und unsere Rolle in der Gesellschaft, sondern auch die Anforderungen an unsere IT-Sicherheit – ein Bereich, der lange unterschätzt wurde. Die Folge ist eine schnell wachsende Zahl von Angriffen auf Universitäten.

Die richtige Balance zwischen ausreichender Sicherheit und Bewahrung des Wesens einer Universität zu finden, bleibt eine ständige Aufgabe – eine, die mich nachts wachhält, mich aber morgens auch motiviert aufstehen lässt.

Vielen Dank für Ihre Zeit und Aufmerksamkeit, ich freue mich auf Fragen und die

Diskussion.