«Digital World»

Chancen und Gefahren des technischen Wandels erkennen und die Zukunft mitgestalten

Ein Gastbeitrag von Dr. Esther Hefti und Grégoire Hernan

Moderiert wurde der Event mit den vielfältigen Referenten professionell von Erich Hofer, CIO BVE Kanton Bern.

Am Mittwoch 11. September 2019 lockte dieses Jahr nebst einem reich befrachteten Programm auch ein vielversprechendes online Experiment, bei welchem sich die Teilnehmenden interaktiv am Geschehen beteiligen konnten. Diese Möglichkeit wurde rege genutzt, indem in Echtzeit Fragen zu den Präsentationen gestellt sowie an Umfragen teilgenommen werden konnte.

Als erster Referent stellte **Sascha Tarli**, Rechtsanwalt und Leiter Zentrale Koordination Beschaffung des Kantons Bern, unter dem Titel «Digital protected world – What else? » die für Digitalisierungsprojekte rechtlich relevanten Rahmenbedingungen vor. Deren Einhaltung sei gerade im digitalen Zeitalter unabdingbar, um die vom Staat bewirtschafteten Informationen angemessen zu schützen. Er wies dabei auf die Gesetzgebungsbestrebungen des Bundes im Bereich von Datenschutz und Informationssicherheit hin.

Zentral sei bei allen Digitalisierungsprojekten, dass der Schutz der Freiheit des einzelnen vor dem Staat angemessen gewährleistet werde. Hierzu sei unbedingt erforderlich, dass einerseits Juristinnen und Juristen die Grundlagen der ICT verstünden, andererseits aber auch die ICT-Mitarbeitenden die rechtlichen Strukturen und juristischen Besonderheiten einer staatlichen Verwaltung (und damit den Gegensatz zur Privatwirtschaft) kennten. Er illustrierte seine Aussagen mit diversen Beispielen aus der Schnittstelle von ICT und Recht. Insbesondere nannte er Institutionen der interkantonalen Zusammenarbeit, wo teilweise unklar bleibe, wer für den Datenschutz zuständig und verantwortlich sei und welches Recht in Einzelfall zur Anwendung komme. Dies sei problematisch, da der Staat seine Datenflüsse kennen und steuern können und im Ereignisfall auch die Verantwortung dafür übernehmen müsse.

Abschliessend zeigte er eine Vielzahl von Lösungsansätzen auf: Als «Good Public Governance» nannte er bei kantonsübergreifenden Projekten z.B. ausgelagerte Trägerschaften, für welche ausreichende Rechtsgrundlagen bereitgestellt würden, was die demokratische Steuerung und Aufsicht garantiere. Bei Projekten empfahl er für die Initialisierungsphase eine profunde Analyse bezüglich Datenschutz, Informationssicherheit und Rechtsgrundlagen sowie eine Klärung von Kompetenzen und Verantwortungen. Für die Konzeptphase riet er insbesondere, die Datenschutzaufsichtsbehörde rechtzeitig einzubeziehen und ISDS-Anforderungen in der Ausschreibung als Muss-Kriterien zu bezeichnen. Zudem sei für Outsourcing-Verträge ein Muss-Inhalt vorzugeben wie etwa Schweizer Recht oder die Geltung der AGB SIK. Für die Realisierungs- bzw. Einführungsphase seien Technik und Organisation der Informationssicherheit anhand realistischer Übungen zu überprüfen und für die Betriebsphase seien bei jedem Change eine neue ISDS-Analyse und nötigenfalls entsprechende Anpassung des ISDS-Konzepts bzw. der ISDS-Anforderungen nötig. Schliesslich sei mit Audits das Funktionieren von Organisation und Technik regelmässig zu überprüfen.

Als Pendant plädierte **Matthias Stürmer** von der Uni Bern unter dem Titel «Digital open world» für eine offene Verwaltung. Er nannte als Beispiele dafür das Öffentlichkeitsprinzip (wo der Eidgenössische

Datenschutz- und Öffentlichkeitsbeauftragte sowohl für Transparenz als auch für Privatsphäre zuständig sei), Open Source Software (OSS) und Open Government Data (OGD). Wichtig bei allen diesen Offenheits-Themen sei, dass der Datenschutz eingehalten werde. Namentlich umfasse OGD keine personenbezogenen und auch keine sicherheitsrelevanten Daten.

Offenheit sei für alle von grossem Nutzen: Erstens werde damit die Transparenz über staatliches Handeln erhöht, was bessere Entscheidungsgrundlagen und Vertrauen in die Technologie schaffe. Zweitens werde damit die Zusammenarbeit über alle Staatsebenen hinweg gefördert. Drittens werde damit Innovation unterstützt, viertens würden damit Kosten gespart (Stichwort Vendor Lock-In). Fünftens würde damit die Unabhängigkeit erhöht, indem eine Abhängigkeit insbesondere auch von amerikanischen und chinesischen Unternehmen verhindert werde. Ziel der digitalen Nachhaltigkeit sei, den Nutzen der Digitalisierung für die gesamte Menschheit von heute und morgen zu maximieren. Voraussetzungen dafür seien: Ausgereiftheit von digitalen Gütern (wie hohe Qualität), transparente Strukturen (wie offen zugänglicher Software-Quellcode), semantische Daten, verteilte Standorte, freie Lizenzen und geteiltes Wissen (was die Abhängigkeit von einzelnen Personen, Firmen oder Organisationen reduziere) eine Partizipationskultur und faire Führungsstrukturen sowie schliesslich eine breit abgestützte Finanzierung.

Die anschliessende Fragerunde zu beiden Referaten wurde rege genutzt und betraf die unterschiedlichsten Themen von Ökologie bis Gesetzgebung.

Marco Grzybeck von Symantec sprach nach der Pause unter dem Titel «Aktuelle Bedrohungslage in der digitalen Welt» über die derzeit zu beobachtenden Angriffsstrategien. Auffallend sei, dass die Angriffe heute eine hohe Professionalität aufwiesen und sehr lukrativ seien (mehr als der Drogenhandel). Gleichzeitig zeige sich, dass sich die Angreifenden in einem richtigen Anstellungsverhältnis (von kriminellen Organisationen oder gewissen Staaten) befänden und somit reguläre Arbeitszeiten und beispielsweise freie Wochenenden hätten. Auch könnten bei solchen Angriffen einzelne Arbeitsschritte outgesourct werden, und es gebe Support.

Die Angriffe selber seien eher einfach ausgestaltet, dafür aber sehr zahlreich; es genüge nämlich, wenn von unendlich vielen Angriffen ein einziger nicht abgewehrt werde. Angriffe erfolgten oft selektiv, indem die Supply-Chain angegriffen werde. Die zielgerichteten Angriffe richteten sich häufig gegen Unternehmen; dies sei lukrativer als beispielsweise bei Privaten die Daten zu blockieren und dafür kleine Summen zu erpressen. Viele Angriffe seien ausserdem schwierig zu erkennen, weil das Opfer zuerst ausgespäht werde, wobei relevante Informationen über seine Systeme und allfällige Schwachstellen gesammelt würden. Angriffe erfolgten immer noch vielfach über Mail (in der Schweiz habe von 333 Mails eines Malware). Eine Angriffsart sei auch, Malware in Patches von Software-Updates hineinzubringen; solche Patches würden nämlich nicht auf Schadsoftware gescannt. Eine wichtige Rolle spiele ebenfalls das Social engineering.

Abschliessend empfahl der Referent, um nicht Opfer eines Angriffs zu werden, ein regelmässiges Backup zu machen, gute Passwörter (insbesondere mit Multifaktor-Authentifikation) zu verwenden, VPN zu benutzen, nicht jedem WiFi-Hotspot zu vertrauen, regelmässige Software-Updates zu machen und nicht alles zu glauben, was man sehe und lese sowie zwei Mal zu überlegen, bevor Software und Devices installiert würden.

In der Fragerunde wurde unter anderem auf die Wichtigkeit der Zusammenarbeit angesichts der modernen Bedrohungen hingewiesen.

Benedikt Ahlfeld, Autor und Unternehmer, stellte anschliessend die Generation Zombie vor. Sie sei sehr stark aufs Handy fixiert. Dennoch sei sie für den Arbeitsmarkt wichtig, da bereits heute 30% der Unternehmen einen Engpass an Nachwuchs-Führungskräften sähen. Die Generation Z hätte eine selektive Wahrnehmung und kurze Aufmerksamkeitsspannen, weshalb man sie anders ansprechen müsse. Sie sei aber auch sinn- und werteorientiert und könnte «hinter die Kulissen» sehen. Sie pflege zwar eine bedachte Selbstdarstellung, aber ebenfalls traditionelle Werte wie Familie und (auch virtuelle) Freunde. Bei ihnen stehe Lebenslust-Maximierung der finanziellen Sicherheit gegenüber, das Verantwortungsbewusstsein der Illoyalität, wenn sie ihre Werte verraten fühlten. Zwar habe sie eine schnelle Auffassungsgabe, jedoch wegen der kurzen Aufmerksamkeitsspannen auch weniger Durchhaltevermögen.

Bei der Generation Z sei eine höhere Fluktuationsrate festzustellen; sie wolle immer mal wieder etwas Anderes ausprobieren und habe Mühe mit festgefahrenen Strukturen. Dafür bringe sie bezüglich Innovation, Schnelligkeit und Flexibilität ein grosses Potential mit und stehe auch für Loyalität und Stabilität (solange sie einen Sinn darin sehe). Mit der grösseren Fluktuation sei zudem ein erhöhter Wissenstransfer verbunden, da von früheren Stellen bereits viele Kompetenzen mitgebracht würden. Daraus folgerten als Handlungsempfehlungen: Es müssten flexible Arbeitszeitmodelle angeboten werden, das Unternehmen müsste Werte und eine Mission kommunizieren, aber den Mitarbeitenden auch Wertschätzung geben und ihnen Verantwortung übertragen. Die Organisation sollte virtuell sein, indem eigenständiges und selbstbestimmtes Arbeiten in einer gemeinschaftlichen Atmosphäre ermöglicht werde (Bürokratie sei dagegen zu vermeiden). Dazu kommte eine transformationale Führung, d.h. Führungspersönlichkeiten mit Vorbildcharakter, die ihren Untergebenen auch wichtige Aufgaben zutrauten. Schliesslich müsse eine Gesundheitsförderung verwirklicht werden, und zwar nicht nur im Büro. Als Fazit empfahl der Referent, die Generation Z nicht vorschnell zu verurteilen.

In der Fragerunde wurde unter anderem diskutiert, ob die Handlungsempfehlungen auch für die öffentliche Verwaltung funktionierten; dies sei zu bejahen sei, da Innovation, Kreativität und Verbindung zur digitaler Welt der Generation Z neue Impulse positiv Einfluss nehmen könnten.

Nach dem Mittagessen sprach **Martin Andenmatten** von Glenfis über die Rolle, welche die interne IT-Organisation in der digitalisierten Zukunft noch einnimmt. Die künftige Welt lasse sich als volatil, unsicher und komplex charakterisieren. Niemand wisse mehr, wie ein Dienst von A – Z funktioniere. Vieles sei mehrdeutig, weshalb Standards out seien. Dabei müssten viele neue Technologien beherrscht werden können. Die Arbeitsmethoden seien agil, und dabei müsse erst noch alles schneller, besser und billiger gemacht werden.

Die Wertvorstellungen im Unternehmen und deren Zusammenarbeits-Kultur würden sich ändern: Statt Profit stehe der Zweck im Vordergrund, statt Hierarchie das (selbst organisierte) Netzwerk, statt Kontrolle Befähigung, statt eines Plans der Versuch und statt der Privatsphäre die Transparenz. Das Business wolle von der technischen Entwicklung profitieren: beispielsweise würden Applikationen und Dienste aus der Cloud bezogen und die Mitarbeitenden würden sich selber durch BYOD behelfen. Heute bestünden viele isolierte Dateninseln mit wenig Transparenz und ohne jegliche Sicht auf die Gesamtzusammenhänge. Eine solche Welt sei schwer zu digitalisieren. Deshalb sollten wir wegkommen vom «We can all» und stattdessen das Nötige kaufen, aber diese Lösungen implementieren und später orchestrieren. Damit würden die Aufgaben immer anspruchsvoller, namentlich auch im Hinblick auf die Compliance. Wegkommen sollte man ebenfalls vom Silo-Denken.

Zentral seien die Grundsatzfragen: Was will man selber machen und was outsourcen? Wie will man sich in Zukunft positionieren? Auf welchem Level ist das Business jetzt? Denn je nachdem, wie diese Fragen beantwortet würden, brauche es eine andere IT-Organisation. Dabei lasse sich das Level 1 charakterisieren mit «Ad hoc» (wer am lautesten schreit, bekommt zuerst etwas), Level 2 als «Order Taker», Level 3 als «Service Provider», Level 4 als «Trusted Advisor» und das oberste Level 5 als «Strategic Partner». Als Vision sollte eine ganzheitliche Zusammenarbeit und konsequenterweise ein integriertes IT-Betriebsmodell über den gesamten Service Lifecycle hinweg bestehen. Dabei sei indessen erforderlich, dass die IT das Business, seine Anforderungen, Bedürfnisse und Wünsche verstehe. Damit wurde klar, dass es die IT-Organisation der Zukunft zwar noch braucht, aber nicht mehr als Order-Taker, sondern als stragischer Business-Partner.

Die Fragerunde drehte sich insbesondere darum, dass statt des Selber-Machens vermehrt Lösungen angeboten werden sollten.

Dordaneh Arangeh von der ETH Zürich zeigte in ihrem Referat als erstes, dass IT-Organisationen selbst am meisten von der Digitalisierung betroffen sind; sie müssen Entwicklungen unterstützen, welche ihr Arbeitsleben am meisten verändern und ihre heutige Daseinsform in gewissen Bereichen sogar in Frage stelle. Als Beispiel eines äusseren Faktors der neuen Spielregeln mit sich bringt, nannte sie die Änderung der Software-Lizenzierung auf userbasierte Modelle. Wenn Mitarbeitende und Studierende vermehrt mit eigen beschafften End-Devices arbeiten, sie für die Beschaffung einer Software lediglich eine gültige Mail-Adresse des Unternehmens resp. der Universität benötigen, wird ein zentrales Software-Asset-Management zur Illusion. An der ETH bestehe zusätzlich eine besondere Situation, indem jede Professur ein eigenes Start-up darstelle, dass ihr Budget individuell verwalte und dieses durchaus auch für eigene IT investieren darf. Vor diesem Hintergrund stellte Dordaneh Arangeh die Frage, wie lange es ITSM und den IT-Support in der heutigen Form zukünftig noch geben wird. Anhand von fünf Thesen zur Zukunft des IT Service Managements und des IT Supports versuchte sie aufzuzeigen, welchen Herausforderungen sich eine interne IT Organisation in Zukunft stellen muss.

These 1: Die IT wird zur App - Moderne ITSM-Lösungen erlauben Prozessautomatisierung auf hohem Niveau. Sich häufig wiederholende Aufgaben (u.a. Ein-/Austritt von Mitarbeitenden) werden vermehrt automatisiert. Neue Mitarbeitende bekommen künftig eine Message auf ihr End-Device. Der dort enthaltene Link führt zu einer App. Nach deren Installation sehen sie einen Servicekatalog mit allen Applikationen und Services, die die IT für sie in ihren Rollen und in ihrem Aufgabengebiet freigegeben hat. Einige sind gem. Rolle vorgegeben, andere sind nach Belieben wählbar.

These 2: Empowering users to enable business – Mitarbeitende beziehen ihre Software vermehrt über Self-Service-Portale, rund um die Uhr. Laufen wissenschaftliche Experimente über das Wochenende und der Speicherplatz wird knapp, so muss dieser ad-hoc und ohne Interkation mit der IT Organisation vergrössert werden können.

These 3: KI unterstützt den Service Desk - Um eine Störung zu melden, muss der Endanwender nicht mehr beim Helpdesk anrufen oder ein Incident Ticket erstellen. KI in Form virtueller Assistenten und Chatbots wird dem Service Desk vorgeschaltet sein: Die KI nimmt dem Service-Desk jene lästigen Routineabläufe ab, die das Arbeiten im First Level Support so unbeliebt machen.

These 4: Omnichannel IT Coaching - Die traditionellen Support-Tiers (1st-3rd Level-Support) verlieren ihre Gültigkeit, da die Grenzen zwischen den Tiers immer mehr verschwinden. Help-Yourself unterstützt von Peers und KI (Chatbots, Knowledge-Bases) wird vermehrt der erste Schritt für die

Problemlösung werden. Der IT-Supporter ist dabei nur noch ein Element von vielen und er wird somit zum IT-Coach, der den Endanwender befähigt, Probleme mit verschiedenen Hilfsmitteln aus verschiedenen Kanälen selber zu lösen.

These 5: ITSM ist strategischer Partner und Service Broker - Die interne IT steht im Wettbewerb mit Cloud Service Providern. Viele Fachabteilungen beziehen IT Services und Apps direkt aus der Cloud – die interne IT-Organisation nennt das „Schatten-IT", aus Sicht der Mitarbeitenden ist es aber schlicht „modernes Arbeiten". Die interne IT nutzt zukünftig ihren Servicekatalog, um Endanwendern das Beste aus beiden Welten anzubieten – aus einer Hand, benutzerfreundlich. Eine der wichtigsten Aufgaben im IT Service Management der Zukunft wird darin bestehen, ein Nutzen bringendes Service Brokerage aufzubauen.

Dordaneh Arangeh ist überzeugt: nur wenn sich die interne IT diesen Herausforderungen stellt, wird sie letztendlich zu einem strategischen Business-Partner. Bereits heute haben die Informatikdienste der ETH ihre IT so umgestaltet, dass ein Framework zur Verfügung steht, über das sich Prozesse automatisieren lassen und Dienstleistungen im Self-Service-Portal angeboten werden können, inkl. eines mächtigen Reportings, anhand dem zukünftige Entwicklungen besser prognostiziert werden können.

Die an das Referat anschliessende Fragerunde führte zu angeregten Diskussionen, insbesondere auch über die Frage, wie die Endkundinnen und –kunden (Mitarbeitende und Studierende) an der ETH in die Entwicklungsprozesse einbezogen worden seien. Da eine direkte Involvierung von knapp 10'000 Mitarbeitenden und über 20'000 Studierenden nicht möglich sei, seien dazu Erfahrungswerte genommen und gezielte Umfragen durchgeführt worden.

Als nächstes informierte **Cyril Hollenstein** von Microsoft unter dem Titel «Hyperscale Cloud-Computing auch in der Schweizer Verwaltung? », dass vor kurzem im Inland zwei neue Datencentren eröffnet worden seien (das eine in der Nähe von Zürich und das andere bei Genf). Damit seien die Anforderungen von Compliance, Data Residency und Performance auch für anspruchsvolle Applikationen erfüllt. Auch im Desasterfall blieben die Daten in der Schweiz. Bereits jetzt stehe ein Azure Grundangebot zur Verfügung; weitere Schritte würden folgen. Office 365 werde in drei bis sechs Monaten bereitstehen. Für den Betrieb der physischen Infrastruktur in der Schweiz sei eine eigene lokale Organisation gegründet worden, deren Mitarbeitende Schweizer Recht unterstellt seien. Microsoft garantiert zudem vertraglich die Einhaltung des Schweizer DSG. Bereits sei das Projekt unter dem Motto «Services statt Server» mit unterschiedlichster Schweizer Kundschaft aus der Verwaltung gestartet. Die Schweizer Verwaltungslandschaft sei demgegenüber noch ziemlich heterogen in ihrer Haltung zur Cloud. Zwecks Erfahrungs- und Know-how-Austausches wird ist deshalb ein «Schweizer Government Cloud Gremium» ins Leben gerufen worden, an dem alle teilnehmen könnten, welche die Idee unterstützten.

Die intensiv genutzte Fragerunde befasste sich vor allem mit dem Preis, welcher für Azure Services aus den CH-Datacentern 20% teurer sein werde als aus den beiden europäischen Hauptregionen Dublin/Amsterdam (für Office365 wird keine Preisdifferenz erwartet), sowie mit der Frage der Supportorganisation/Supportzugriffe, welche eine neue Betrachtung aus Sicht der Prozesse und technologischen Möglichkeiten erfordert damit Compliance Anforderungen eingehalten werden können (als Beispiel wurde hier die «Customer Lockbox» erläutert).

Anschliessend skizzierte **Zbynek Svoboda** von Swisscom den Arbeitsplatz der Zukunft. Auszugehen sei von der Tatsache, dass die Prozesse immer schneller abliefen und die Auswahlmöglichkeiten immer vielfältiger würden, weshalb eine schnelle und gute Entscheidung zur Erfolgswährung werde. Die Menschen würden daher alles lieben, was die Realität vereinfache. Sie seien zudem ziemlich erfahren, welche Informationen sie glauben könnten und welche nicht, und sie wüssten auch, wo sie Zusatzinformationen finden würden.

Das Potential der digitalisierten Gesellschaft liege in der Stimulierung und Vernetzung der Intelligenzen. Zentral sei daher in Zukunft ein Lifestyle-Arbeitsplatz, wo zeitlich und örtlich flexibel zusammengearbeitet werden könne. Zudem sei ein Low-impact Arbeitsplatz wichtig, wo neben den potentiellen finanziellen Kosten und auch die klimabedingten Risiken zum Standard der Berichterstattung gehörten (virtuelles Zusammenarbeiten ersparten das Pendeln sowie das Reisen). Von Bedeutung sei des Weiteren ein mit künstlicher Intelligenz versehener intelligenter Arbeitsplatz sowie ein grenz- und generationenübergreifender Arbeitsplatz. Es komme also darauf an, die richtigen Dinge richtig zu tun. Hierzu biete sich das Target Operating Model (TOM) an. Auf der Nachfrageseite stünden Begriffe wie AnyWhre, AnyThing, AnyDevice, AnyTime und AnyOne, auf der Angebotsseite Begriffe wie Identitäten, Geräte, Netzwerk, Daten, Anwendungen und Infrastrukturen. Für die IT bedeute diese Methode, erstens ein klares Bild von der bewirtschafteten IT zu haben und über den aktuellen Stand genau informiert zu sein, zweitens die Anforderungen in Bezug auf Services, Mitarbeitende, Prozesse und Technologien zu kennen und die Strategie darauf auszurichten, drittens mit Hilfe der detaillierten Roadmap jederzeit und stufengerecht erklären zu können, wo die ICT Reise hin gehe und viertens, je Service mit indikativen Preisen zeitgerecht die notwendigen Mittel beantragen und begründen zu können. Bei einer Änderung der Business-Strategie könne TOM zudem einfach angepasst werden.

Als letzter Referent der Veranstaltung gab **Thomas Wenk** von der Stadtpolizei Zürich unter dem Titel «Kehrseiten der Digitalisierung» einen Einblick in die Arbeit der digitalen Ermittlungsdienste. Diese Mitarbeitenden seien zuständig zur Beschlagnahmung von Computern, zur Ermittlung im Internet/Darknet, zum Knacken von Passwörtern und zum Auslesen von Daten aus technischen Geräten (wie z.B. Überwachungskameras, Drohnen, Kühlschränken), welche bei Delikten involviert gewesen seien. Für ihre Auswertungen setzten sie dabei eigene Software ein. Bei der operativen Kriminalanalyse werde sodann mittels Geoprofiling abgeschätzt, wann und wo der nächste Einbruch mutmasslich stattfinden werde. Beteiligt seien sie auch am Cybercrime Kompetenzzentrum, das gemeinsam von Stadt und Kanton betrieben werde. (Leider gebe es in diesem Bereich viele Hürden juristischer Natur.) Erfolgreich bekämpft werden könne Cyberkriminalität dabei nur, wenn landes- und kontinent-übergreifend sowie global und agil zusammengearbeitet werde.

Schliesslich schilderte der Referent anschaulich konkrete Beispiele von Cyber-Attacken aus seiner Praxis. So sei ein Angriff mit einem gefälschten Mailabsender ausgeführt worden (z.B. zuerích statt zuerich in der Mailadresse). Aus den geschilderten Beispielen folgerte er, dass bei den betroffenen Stellen eine lernfördernde Fehlerkultur gepflegt werden sollte: wer einen Fehler gemacht habe, dürfe nicht durch Bestrafung abgeschreckt werden, sondern müsse motiviert werden, auch künftig möglichst schnell eine Meldung zu machen, denn nur so könnten frühzeitig Gegenmassnahmen eingeleitet werden.

Eine typische Cyberattacke folge zurzeit dem Schema, dass das Opfer erst beobachtet und dann die Tat vorbereitet werde. Sodann gebe sich der Angriff technisch zu erkennen und es würden Forderungen gestellt und schliesslich das Lösegeld kassiert. Nach Zahlung der geforderten Summe seien die «gekaperten» Daten und Systeme entweder wieder verfügbar oder sie blieben unwiderruflich verloren. Der Unterschied zwischen potentiellen Opfern sei, wie gut ein solches auf den Eintretensfall vorbereitet sei und wie gut es damit umgehen könne.

Die Fragerunde war sehr lebhaft; gefragt wurde namentlich nach der Zusammenarbeit mit dem European Cybercrime Center; hier funktioniere die Zusammenarbeit noch nicht reibungslos, da der Bund und vor allem das VBS immer noch in Landesgrenzen denke.