#UpdateDE

Microsofts Ideen zur Bundestagswahl 2017 und **für die digitale Transformation** Deutschlands

Microsoft

Firewall-Update: Mit Sicherheit digital

Auszug aus unserer Veröffentlichung #Update DE.
Das gesamte Papier finden Sie unter aka.ms/update-de

Cybersicherheit hat sich vom Nischen- zum Titelthema entwickelt. Schlagzeilen von Cyberkriegen und Erpressungstrojanern zeigen, wie sehr die Herausforderungen der Absicherung von IT-Systemen nicht nur im Unternehmens-, sondern auch im Alltag der Nutzer angekommen sind. Angriffe auf elektronische Wahlsysteme und IT-gestützte Angriffe mit dem Ziel der Beeinflussung von Wahlen rücken die Problematik gar in die Herzkammer der Demokratie.

Gleichzeitig stehen wir mit der Ausbreitung des Internets der Dinge erst am Anfang der Komplexitätsexplosion, wenn es um Sicherheitsfragen geht. Berichte zeigen, wie das rasante Wachstum der Zahl ans Internet angeschlossener – häufig schlecht gesicherter – Endgeräte zum Ausgangspunkt völlig neuer Formen koordinierter Angriffe wird.

Politisch und gesetzgeberisch wurde in den vergangenen Jahren auf vielen Ebenen reagiert: Deutschland hat das IT-Sicherheitsgesetz und eine umfassende Cybersicherheitsstrategie beschlossen. Auf EU-Ebene wurde die NIS-Richtlinie (Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen) verabschiedet. Im Verteidigungsbereich erleben wir eine grundlegende Strukturreform, mit welcher erstmals dem Cyberraum als eigenständigem militärischen Operationsgebiet Rechnung getragen wird.

All diese Bemühungen sind uneingeschränkt zu begrüßen. In den nächsten Jahren wird es nun darum gehen, diese Bemühungen mit Leben zu füllen. Sicherheitsstrategien

müssen in der Breite der Wirtschaft und beim Verbraucher ankommen. Neue global vereinheitlichte Sicherheitsstandards müssen etabliert werden. Microsoft ist überzeugt, dass Cloud-Dienste hier einen zentralen Beitrag leisten können, indem sie neueste Sicherheitstechnologien und die dahinterstehende Analyseintelligenz zugänglich machen. Politisch muss dies gefördert werden, indem die bestehende Fragmentierung von Standards und Zertifikaten reduziert wird und international akzeptierte Normen verabschiedet werden.

„Microsoft is right: We need a Digital Geneva Convention."

Heidi Tworek, Assistant Professor in International History at the University of British Columbia

➡ WIRED online

Hinzukommen müssen verstärkte internationale Bemühungen mit dem Ziel der Einhegung potenzieller zwischenstaatlicher Auseinandersetzungen im Cyberraum. Staatlich initiierte Cyberangriffe und die hierfür eingesetzten Cyberwaffen treffen fast immer zuerst zivile Institutionen. Microsoft setzt sich daher für eine Digitale Genfer Konvention ein, die erstmals bindende zwischenstaatliche Regelungen zum Schutz aller betroffenen zivilen Individuen und Institutionen vorsieht und durch selbstbindende Leitlinien der globalen IT-Wirtschaft in Bezug auf staatlich initiierte Konfliktlagen im Cyberspace ergänzt wird.

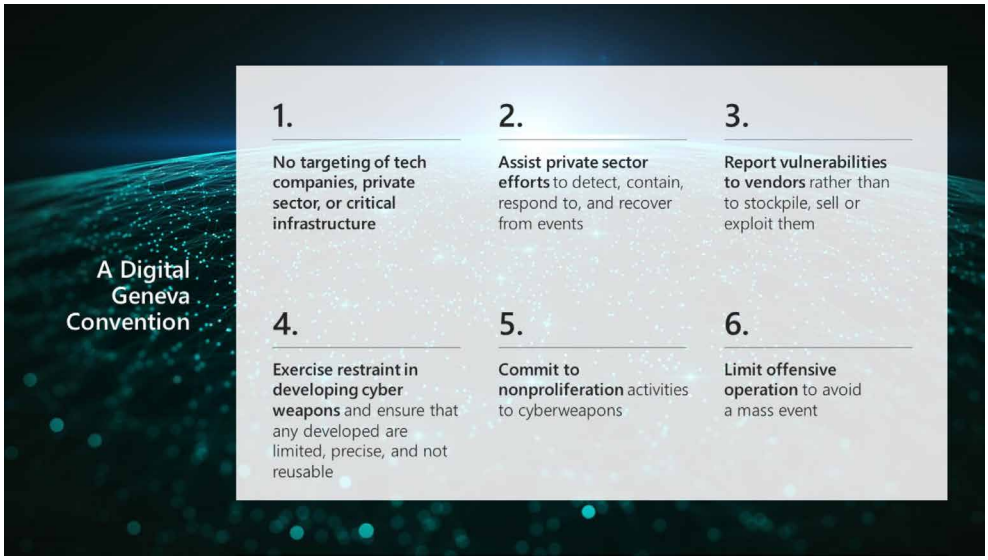
Handlungsempfehlungen

Schaffung einer Digitalen Genfer Konvention

- Microsoft setzt sich dafür ein, die bereits bestehenden Bemühungen zur Einhegung zwischenstaatlicher Konfliktlagen im Cyberspace zu intensivieren und eine Digitale Genfer Konvention mit Ziel des Schutzes ziviler Institutionen im Internet zu beschließen. **So wie die internationale Staatengemeinschaft 1949 zusammenkam, um gemeinsame Maßnahmen zum Schutz von Zivilisten in Kriegszeiten zu vereinbaren, brauchen wir eine Digitale Genfer Konvention zum Schutz ziviler Institutionen bei zwischenstaatlichen Aktivitäten im Cyberraum in Friedenszeiten.** Ergänzt werden soll die Digitale Genfer Konvention durch selbstbindende Leitlinien der globalen IT-Industrie sowie eine neue unabhängige Organisation zur Identifizierung der Verursacher schwerwiegender internationaler Cyberattacken.

➡ *Videolink: Rede von Brad Smith bei der RSA Conference 2017*

- Aufbauend auf bestehenden Initiativen wie der ➡ UN Group of Governmental Experts und der ➡ Global Commission for the Stability of Cyberspace soll eine Digitale Genfer Konvention erstmals bindende Standards für staatliche Aktivitäten im Cyberspace in Friedenszeiten schaffen. Kernelemente dieser Konvention sollten unter anderem sein:



  - Keine staatlichen Angriffe auf kritische Infrastrukturen, deren Ausfall die Sicherheit der Zivilbevölkerung beeinträchtigen würde.
  - Keine Angriffe auf persönliche Daten oder Online-Konten von Journalisten oder privaten Personen im Rahmen von demokratischen Wahlen.
  - Klare Regeln mit Bezug auf staatliche Sammlung, Einsatz, Sicherung und Meldung von IT-Sicherheitslücken, insbesondere im Verhältnis zum betroffenen Anbieter.

- Zwischenstaatliche Regeln zur Eindämmung der Ausbreitung von Cyberwaffen nach dem Vorbild der Abkommen zu konventionellen Waffen.

- Verpflichtung, keine Hintertüren in kommerzielle Massenmarktprodukte einzubringen bzw. zu erzwingen.

- **Parallel zur Digitalen Genfer Konvention aufseiten der Staaten setzen wir uns für selbstbindende Standards der internationalen IT-Industrie ein, den sog. Tech-Accord.** Aufbauend auf dem Grundprinzip 100 % defensiv und 0 % offensiv sollte die globale IT-Wirtschaft Regeln zu ihrer eigenen Rolle im Falle zwischenstaatlicher IT-Angriffe geben. Wir schlagen folgende Grundprinzipien als Ausgangspunkt des Tech-Accord vor:

  - Keine Unterstützung offensiver Operationen jeglicher Staaten.

  - Verpflichtung zum Schutz aller Kunden insbesondere im Falle bekannt gewordener Sicherheitslücken.

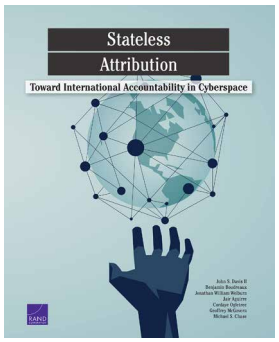
  - Sektorübergreifende Zusammenarbeit zur Abwehr staatlich initiierter offensiver Operationen im Cyberraum.

  - Unterstützung staatlicher Initiativen zur Erkennung und Eindämmung von Cyberangriffen bzw. zur Verringerung deren schädlicher Auswirkungen.

  - Verpflichtung zur gemeinsamen Bekämpfung des globalen Handels mit Sicherheitslücken.

- Die skizzierten Bemühungen sollten schließlich abgerundet werden durch den **Aufbau einer neuen, unabhängigen Institution zur verlässlichen Identifizierung der Verursacher internationaler Cyberangriffe, einem sog. Attribution Council**. Die Beweisspuren digitaler Angriffe sind heute in der Regel weltweit verteilt über Telekommunikationsnetzbetreiber, Service-Provider und die eigentlich Betroffenen. Ihre Analyse erfordert ein Höchstmaß an technischem Sachverstand. Gleichzeitig ist die verlässliche und international akzeptierte Verursachungszuweisung für Cyberangriffe Voraussetzung für adäquate politische Reaktionen. Deshalb setzen wir uns für eine streng unabhängige, unpolitische und technisch fokussierte Organisation zur Identifizierung in Fällen schwerer internationaler Angriffsszenarien ein.

Denkbare Ausgestaltungsmöglichkeiten für ein Attribution Council hat der RAND Thinktank im Auftrag Microsofts untersucht. Der Report „Stateless Attribution – Toward International Accountability in Cyberspace" kann als ➡ E-Book frei im Internet bezogen werden.*

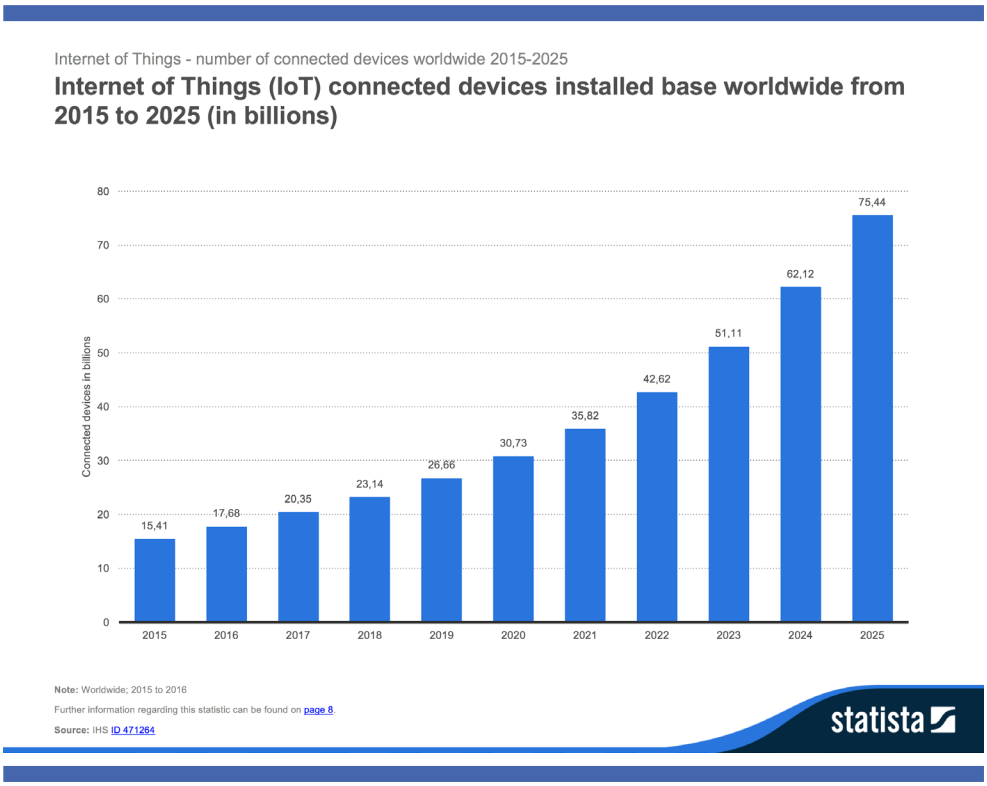


*RAND: Research ANd Development – de.wikipedia.org/wiki/RAND_Corporation

Handlungsempfehlungen

Sicherheit im Internet der Dinge

- IT-Sicherheit ist in Zeiten von Industrie 4.0 und des Internet of Things längst keine exklusive Anforderung an IT-Unternehmen mehr. Wo mehr und mehr Gegenstände des Alltags vernetzt sind, wird IT-Sicherheit zur Querschnittsanforderung für die komplette Wirtschaft vom Kleinunternehmer bis zum Großkonzern. Bot-Netz-Angriffe unter Ausnutzung von IoT-Endgeräten zeigen, dass die Gefahr real ist. Microsoft regt an, zu prüfen, wie die IT-Sicherheit vernetzter Produkte, insbesondere im Verbraucherbereich, erhöht werden kann. Ein denkbarer Ansatz ist die **Etablierung europaweit einheitlicher Mindeststandards für IoT-Produkte bzw. die Einführung von IoT-Sicherheits-Labeln**.



- Momentan fehlt es bei vielen digitalen Produkten und Dienstleistungen an handhabbaren risikobasierten IT-Sicherheits-Mindeststandards. **Microsoft setzt sich für international harmonisierte Mindeststandards für vernetzte Produkte, insbesondere im Bereich des Internet of Things ein.** Vor allem für das Basis-IT-Risikomanagement bedarf es einer stärkeren internationalen Harmonisierung. Hierbei gilt es, die Anschlussfähigkeit an etablierte technische Standards wie z. B. ➡ ISO 27001, den ➡ Datenschutzstandard für Cloud-Dienste ISO 27018 sowie die bereits weit verbreiteten Standardisierungsansätze des ➡ National Institute of Standards and Technology (NIST) zu berücksichtigen.

- **Künstliche Intelligenz und Machine Learning bieten Potenziale zur Erhöhung der IT-Sicherheit durch selbstlernende Schutzsysteme.** Microsoft tritt dafür ein, dass die rasanten technologischen Entwicklungen in diesem Bereich genutzt werden. Wir regen die Einrichtung einer neuen Task Force des Bundesamts für Sicherheit in der Informationstechnik an, die sich in Zusammenarbeit mit dem Deutschen Forschungszentrum für künstliche Intelligenz (DFKI) und unter Einbeziehung aller relevanten Stakeholder mit den Potenzialen maschinellen Lernens für IT-Sicherheitsfragen befasst.

IMPRESSUM

HERAUSGEBER
Microsoft Deutschland GmbH
Unter den Linden 17
10117 Berlin

TEXTVERANTWORTUNG
Dr. Guido Brinkel

HERSTELLUNG
Pressedienst Krawinkel

GESTALTUNG & LAYOUT
Tim Wendland Grafik

LEKTORAT
Schlussredaktion Hamburg

BILDNACHWEIS
Microsoft Corporation
S. 5 © iStock.com/grandeduc
S. 7 © iStock.com/joci03
S. 11 © iStock.com/imarako85