acatech

HORIZONTE

Cyber Security

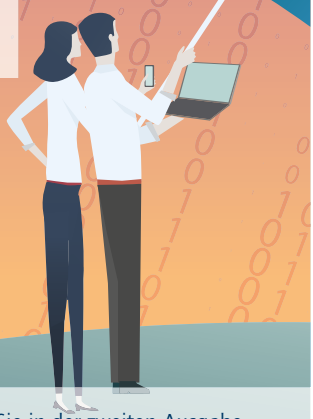
AUF EINEN BLICK

Warum Cyber Security?

Gefährdungsfelder in wichtigen Lebensbereichen

Cyber Security in Deutschland und im internationalen Vergleich

Handlungsfelder und Gestaltungsspielräume



Diese und weitere Informationen erhalten Sie in der zweiten Ausgabe „Cyber Security" der Publikationsreihe acatech HORIZONTE unter: *www.acatech.de/horizonte-cybersecurity*

acatech
DEUTSCHE AKADEMIE DER TECHNIKWISSENSCHAFTEN

Neun Kernbotschaften

1. Weltweit nehmen Cyberangriffe an Vielfalt und Gefährdung rapide zu. In der digital vernetzten Welt werden IT-Systeme so komplex, dass die Risiken nur noch schwer abschätzbar sind: Eine einzige Schwachstelle reicht Cyberkriminellen, um in ein Gesamtsystem einzudringen und Schaden anzurichten.

2. Die größten Gefährdungsfelder für Deutschlands innere Sicherheit, Wirtschaft und Demokratie sind die Bereiche Gesundheit, Stromversorgung, Industrie 4.0, Smart Home und IoT-Geräte, vernetzte Fahrzeuge und Medien. Diese bedürfen eines besonderen Schutzes vor Manipulationen und Cyberattacken.

3. Deutschland ist in der Forschung zu Cyber Security gut aufgestellt. In den Bereichen Kryptographie, Quantencomputing und Security Engineering (Security by Design), um nur einige zu nennen, zählen deutsche Forschende zur Spitzenklasse.

4. Jedoch fehlt in Deutschland die Umsetzung von Forschungsergebnissen in wirtschaftlich erfolgreiche Sicherheitsprodukte. Aufgrund einer starken Abhängigkeit von Zulieferern aus den USA und Asien haben wir hierzulande wenig Kontrolle über die Sicherheit unserer grundlegenden IT-Infrastrukturen.

5. Die Stakeholder aus Politik, Wirtschaft und Wissenschaft arbeiten teils fragmentiert und parallel. Es bedarf eines funktionierenden Regelkreises, bei dem die Akteure ihr Wissen transferieren und sich im Schadensfall und bei der Ursachenforschung gegenseitig unterstützen.

6. IT-Sicherheit wird oft nicht ernst genommen. Kunden sind nicht bereit, mehr Geld für ein sicheres Produkt zu bezahlen, zumal die Konsequenzen eines unsicheren Produktes zunächst nicht spürbar sind. Hier muss der deutsche Staat Mindestsicherheitsstandards für IT-Produkte und -dienstleistungen einführen, die für alle Unternehmen und Branchen verpflichtend sind.

7. Ein Einfalltor für viele Hackerangriffe ist der Mensch. Vor allem KMU müssen ein kritischeres Bewusstsein für Cyberbedrohungen entwickeln und Mitarbeitende sowie IT-Fachkräfte regelmäßig fortbilden. Auch der deutsche Staat muss für digitale Aufklärung sorgen: An Schulen und Berufsschulen ist Sicherheitsbildung nötig; die Gesellschaft ist über Kampagnen zu sensibilisieren.

8. Die größte Schwachstelle ist jedoch nicht der Mensch, sondern Systeme, die den Menschen nicht ausreichend unterstützen. Es ist nun dringend an der Zeit, stärker in die Entwicklung und Herstellung sicherer Software- und Hardware-Systeme zu investieren, welche die Menschen technisch schützen, ohne ihnen unmögliche Aufgaben aufzubürden.

9. Die Verbreitung von Fake News über das Internet hat eine neue Dimension erreicht. Politisch motivierte Hacker, Terrororganisationen oder Geheimdienste überfluten die Öffentlichkeit mit falschen Informationen, sodass diese nicht mehr zwischen richtig und falsch unterscheiden kann. Mögliche Ziele sind, die Schwächen einer politischen Partei aufzuzeigen oder das gesamte demokratische System zu unterminieren.

Gefährdungsfeld

Smart Home

Ein Hacker dringt in die Überwachungskamera eines Smart Homes ein. Über die Kommunikation der Kamera kann er die Geräteadressen (IP-Adresse) anderer vernetzter Produkte im selben Netzwerk abfangen.

Überwachungskameras sind ein leichtes Ziel für Hacking-Attacken. Oft wird bei der Installation das Standardpasswort beibehalten. Hacker können mithilfe einer im Internet zugänglichen Software das Standardpasswort binnen weniger Sekunden finden.

Zunächst verschafft sich der Hacker Zugriff auf den Smart-Fernseher und infiziert diesen mit Schadsoftware. Über eine Nachricht auf dem Bildschirm verlangt er nun Lösegeld in Bitcoins.

Oft reicht es, wenn sich der Hacker Zugriff auf ein einziges (ungeschütztes) Gerät verschafft. Darüber kann er über alle weiteren (vermeintlich sicheren) Geräte im Smart Home die Kontrolle übernehmen, die selbst nicht angreifbar wären.

Wenige Sekunden später hat der Hacker bereits einen Textbefehl an einen vernetzten Lautsprecher gesendet. Der Lautsprecher wandelt den Text in Sprache um und trägt diesen einem digitalen Assistenten vor. „Alarm ausschalten. Türe öffnen", lautet der Befehl aus dem Lautsprecher.

Digitale Assistenten sind sprachgesteuerte, internetbasierte, intelligente Geräte. Sie übertragen die im Raum gesprochenen Worte digital zum Hersteller, wo die Befehle verarbeitet werden.

Der digitale Assistent leitet das Kommando an die Smart Home-App weiter, welche den Alarm sowie die Eingangstüren steuert. Das Türschloss wird ohne physische Einbruchsspuren geöffnet.

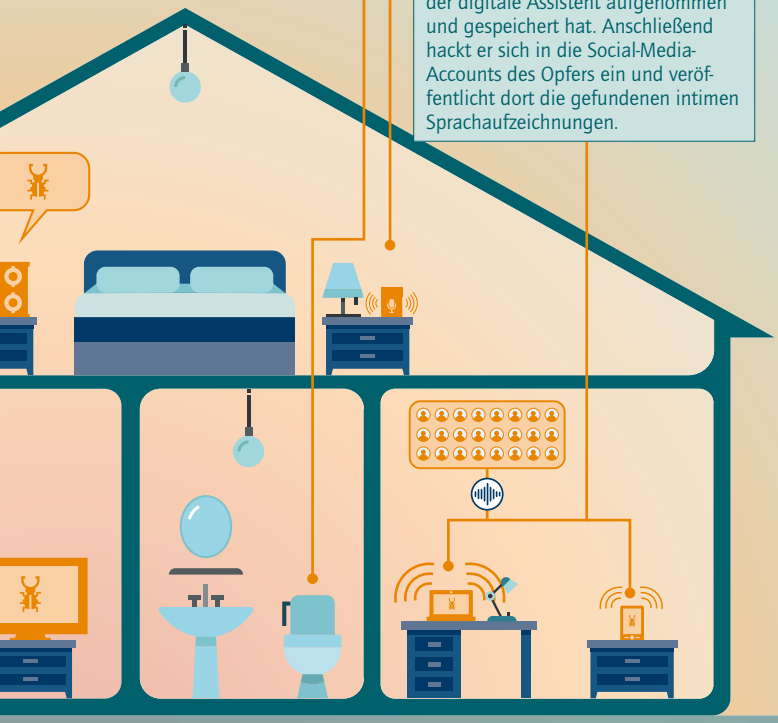
Diese Angriffsfläche gilt als besonders gefährlich: Wenn ein digitaler Assistent und ein Lautsprecher kombiniert Ziel eines Hacking-Angriffs werden, können diese alles, was über Sprachkommandos läuft, neu programmieren.

Als nächsten Sprachbefehl programmiert der Hacker: „Kaufe mir die neueste Drohne". Auch hier leitet der digitale Assistent die Bestellung an einen Online-Lieferanten weiter, der wiederum mit dem Bankkonto des Opfers verbunden ist.

Aus Spaß entscheidet der Hacker, auch in die Nutzungsdaten der Smart-Toilette einzudringen.

Über Nutzungsprotokolle kann er auf sensible Gesundheitsdaten des Toilettenbesitzers zurückgreifen, die sich aus den von der Toilette gesammelten Daten ableiten.

Zuletzt sucht der Hacker nach kompromittierenden Sprachdateien, die der digitale Assistent aufgenommen und gespeichert hat. Anschließend hackt er sich in die Social-Media-Accounts des Opfers ein und veröffentlicht dort die gefundenen intimen Sprachaufzeichnungen.



Quelle: Eigene Darstellung

Was können Einzelne für mehr Sicherheit in

MIT KINDERN/JUGENDLICHEN

- Bedenken Sie, dass Kinder und Jugendliche einfacher als Erwachsene zu beeinflussen sind. Sprechen Sie mit Ihren Kindern über die Verantwortung, die mit der Nutzung sozialer Netzwerke einhergeht. Erläutern Sie Ihren Kindern Datenschutz, Privatsphäre, Informationen im Internet sowie Schutz vor Mobbing.
- Schalten Sie Applikationen ein, die den Zugriff auf bestimmte Funktionen des Telefons regulieren. So bieten Sie Ihren Kindern einen kontrollierten Zugang.

AM ARBEITSPLATZ

- Nehmen Sie an unternehmensinternen IT-Schulungen teil und setzen Sie erworbene Kenntnisse beruflich und privat um.
- Hegen Sie ein gewisses Misstrauen: Klicken Sie nicht alles an, was in Ihrer Mailbox landet.
- Sperren Sie Ihren Bildschirm beim Verlassen des Arbeitsplatzes.
- Notieren Sie sich Ihre Passwörter nicht auf Zettel in der Nähe des Computers.
- Schließen Sie keine unbekannten USB-Sticks an Ihren Computer an. Diese könnten mit schadhafter Software infiziert sein.
- Abteilungen, die keinen Zugriff auf die Daten anderer Abteilungen benötigen, sollen auch nicht unnötig miteinander verbunden sein. Dies kann im Fall einer Cyberattacke die rasche Verbreitung des Angriffs vermeiden.
- Achten Sie auch in der Arbeit auf sichere Passwörter.

IN DEN SOZIALEN MEDIEN

- Begegnen Sie reißerischen, emotional geladenen Artikeln mit Misstrauen: Hacker können über Fake News Menschen manipulieren, verunsichern und die öffentliche Meinung steuern.
- Lesen Sie einen Text genau und prüfen Sie, ob die Information aus einer vertrauenswürdigen Quelle stammt, bevor Sie einen Beitrag teilen.
- Praktizieren Sie laterales Lesen: Öffnen Sie einen weiteren Tab in Ihrem Webbrowser und suchen Sie auf mehreren Nachrichtenportalen nach Berichten zum selben Thema.

n Cyberraum tun?

- Wenn Sie eine Suchmaschine im Internet verwenden, vertrauen Sie nicht darauf, dass die Top-Treffer auch verlässliche Webseiten sind. Suchmaschinen ordnen Ergebnisse nicht nach Wahrheitsgehalt oder nach Seriosität.
- Überprüfen Sie dubiose Meldungen auf sogenannten Faktencheck-Webseiten. Hier bringt die gemeinnützige Presse Fake News ans Licht mit dem Ziel, mehr Transparenz zu schaffen.

ZU HAUSE

- Spielen Sie Software-Updates sofort auf Ihren Rechner, auf Ihr Tablet oder Smartphone. Verschieben Sie dies nicht auf später! Stellt ein Unternehmen ein Update zur Verfügung, können Kriminelle die Sicherheitslücke ausfindig machen und in nur wenigen Stunden über die offene Lücke Ihr Gerät angreifen.
- Halten Sie Anti-Viren- und Firewall-Software unbedingt auf dem aktuellen Stand. Auch hier gilt es, Sicherheitslücken sofort zu schließen.
- Verwenden Sie Passwörter nicht für verschiedene Systeme gleichzeitig. Anderenfalls hat ein Hacker Zugriff auf Ihre weiteren Konten, sobald er eines Ihrer Passwörter geknackt hat. Passwörter sollten möglichst lange und komplex sein. Verwenden Sie, wenn möglich, eine Zwei-Faktor-Authentifizierung.
- Ändern Sie beim Erwerb eines neuen Smart Home-Geräts sofort das Standard-Passwort.
- Laden Sie keine Apps oder Computerprogramme von Webseiten herunter, die nicht vertrauenswürdig sind.
- Bei kostenlosen Apps oder Services sind oft Ihre Daten der Preis.

acatech HORIZONTE

Mit den **acatech HORIZONTEN** möchte die Akademie die Diskussion über neue Technologien anregen, politische Gestaltungsräume aufzeigen und Handlungsoptionen formulieren. Auf diese Weise möchte acatech einen Beitrag für eine vorausschauende Innovationspolitik leisten.

www.acatech.de/horizonte-cybersecurity

MITWIRKENDE

Gesamtleitung acatech HORIZONTE:
Prof. Dr.-Ing. Jürgen Gausemeier, acatech Vizepräsident /Heinz Nixdorf Institut der Universität Paderborn, Seniorprofessor

Konzeption, Text und Experteninterviews:
Christina Müller-Markus, acatech Geschäftsstelle, Innovationsforum (federführende Autorin)

Projektgruppe Cyber Security:
Paul Duplys, Robert Bosch, Leiter Competence Segment Safety, Security & Privacy (Corporate Research)

Prof. Dr. Claudia Eckert, Technische Universität München, Leiterin Lehrstuhl Sicherheit in der Informatik/Fraunhofer-Institut für Angewandte und Integrierte Sicherheit (AISEC), Leiterin

Alexander von Gernler, genua GmbH, Leiter Research/Gesellschaft für Informatik e.V., Vizepräsident

André Grochowy, Munich Re, Senior Cyber Underwriter, Corporate Underwriting

Prof. Dr. Christoph Meinel, Hasso-Plattner-Institut, Institutsdirektor und CEO/Digital Engineering Fakultät – Universität Potsdam, Dekan

Stephan Micklitz, Google Germany, Direktor Engineering

Prof. Dr. Jörn Müller-Quade (Leiter), Karlsruher Institut für Technologie, Leiter der Forschungsgruppe Kryptographie und Sicherheit

Christian Stüble, Rohde & Schwarz Cybersecurity, Chief Technical Officer

Prof. Dr. Michael Waidner, Fraunhofer-Institut für Sichere Informationstechnologie (SIT), Leiter/Technische Universität Darmstadt

Eva Weiß-Margis, T-Systems International GmbH, Telekom Security, Internal Security & Cyber Defense, Vice President Security Officer

HERAUSGEBER: acatech – Deutsche Akademie der Technikwissenschaften

ADRESSEN STANDORTE

Geschäftsstelle
Karolinenplatz 4
80333 München
T +49(0)89/520309-0
F +49(0)89/520309-900

Hauptstadtbüro
Pariser Platz 4a
10117 Berlin
T +49(0)30/2063096-0
F +49(0)30/2063096-11

Brüssel-Büro
Rue d'Egmont/Egmontstraat 13
B-1000 Brüssel
T +32(0)2/213 81-80
F +32(0)2/213 81-89

horizonte@acatech.de
www.acatech.de
https://www.acatech.de/horizonte

Empfohlene Zitierweise:
acatech (Hrsg.): *Cyber Security* (acatech HORIZONTE), München 2019

München 2019 | acatech HORIZONTE
ISSN 2625-9605

acatech
DEUTSCHE AKADEMIE DER TECHNIKWISSENSCHAFTEN