Digitale Vernetzung um jeden Preis?

secunet und deren Mission, uns digital zu schützen

Dr. Kai Martius im Gespräch

Kai Martius ist Chief Technical Officer von secunet, Deutschlands führendem Cybersecurity-Unternehmen. Seit Jahren befasst er sich mit dem bestmöglichen Schutz von Daten, IT-Infrastrukturen und digitalen Identitäten. Secunet hat sich darauf spezialisiert, für besondere Sicherheitsansprüche im Netz zu sorgen – zum Beispiel bei der Geheimhaltung von wichtigen Informationen oder bei der Vernetzung von Produktionsanlagen von Industrieunternehmen. Außerdem sorgt secunet dafür, dass Patientendaten geschützt im digitalen Gesundheitsnetz unterwegs sind und dass Nutzer der elektronischen Steuererklärung ELSTER sich sicher anmelden und zweifelsfrei authentifizieren können. Wo steuern wir mit der digitalen Revolution hin? Und was für einen Preis müssen wir dafür in puncto Sicherheit bezahlen?

„Im Großen spricht man von digitaler Souveränität. Sie ist ein Faktor, der der digitalen Determination entgegenwirkt."

Das Internet ist ein Raum, der prinzipiell keine physischen Grenzen kennt. Wie global sehen Sie das Problem der Internetsicherheit? Wie arbeiten Sie mit der Bundesrepublik Deutschland zusammen? Wie mit noch größeren Institutionen?

Cyberkriminelle oder auch Hacker in staatlichem Auftrag können grundsätzlich von überall auf der Welt angreifen. Bedrohungsszenarien für die Internetsicherheit oder ganz allgemein für die Informationssicherheit müssen wir daher immer global denken. Auch unser Angebot richten wir weltweit aus. Industrieunternehmen profitieren von unseren Lösungen, egal, wo sie ihren Sitz haben. Wir arbeiten für zahlreiche Behörden anderer EU-Staaten. Unsere Wurzeln liegen allerdings klar in Deutschland: Seit 2004 sind wir IT-Sicherheitspartner der Bundesrepublik. Alle Bundesministerien und mehr als 20 DAX-Konzerne zählen zu unseren Kunden.

Und wie steht es um die Sicherheitslage in Deutschland im Vergleich zu anderen EU-Ländern; wie im globalen Vergleich?

Hier muss man differenzieren: Der Bereich der öffentlichen Verwaltung in Deutschland ist hinsichtlich der IT-Sicherheit stark reguliert, für die Bundesverwaltung gelten strikte Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI). Daher wird viel in Cybersicherheit investiert. Das Schutzniveau der Behörden in Deutschland ist entsprechend hoch.

Im weitgehend unregulierten privatwirtschaftlichen Bereich sieht das anders aus: Hier gibt es größtenteils deutliches Verbesserungspotenzial. Das gilt für Deutschland und auch für andere Länder. Ein Sonderfall sind die kritischen Infrastrukturen, zum Beispiel Energie- und Wasserversorger. Cyberangriffe auf diese Betriebe können schwerwiegende Folgen für die gesamte Gesellschaft haben. Daher bestehen in Deutschland seit 2015 gesetzliche Regelungen für die IT-Sicherheit kritischer Infrastrukturen, und folglich ist bei deren Sicherheitsniveau auch ein Aufwärtstrend zu beobachten.

Die Corona-Krise hat viele zum Homeoffice gebracht. Steigen damit auch die potenziellen Gefahren einer Virtualisierung unseres Alltags, der wiederum dadurch lukrativer wird für Verbrechen? Was können wir als User konkret dagegen tun?

Auch mobile Arbeitsplätze können sehr gut abgesichert werden, sodass keine Sicherheitseinbußen gegenüber einem stationären Arbeitsplatz im Büro entstehen. Schon vor der Corona-Krise haben wir das für viele unserer Kunden getan – gerade für solche, die mit besonders schützenswerten Daten arbeiten. Dabei nutzen wir die Sicherheitsarchitektur SINA, die wir ursprünglich im Auftrag des BSI entwickelt haben. Sie besteht unter anderem aus Netzwerkkomponenten, die den gesamten Datenverkehr spionage- und manipulationssicher verschlüsseln, sowie sehr sicheren Clients wie zum Beispiel Laptops. Je nach Gefährdungslage bei dem konkreten Auftraggeber gilt es, ein angemessenes Schutzniveau zu finden, sodass Aufwand und Nutzen in einem gesunden Verhältnis stehen. Wird das Schutzniveau zu niedrig angesetzt, haben Hacker natürlich leichtes Spiel.

Auch als User können Sie eine Reihe von Dingen tun, um unterwegs oder im Homeoffice keine unnötigen Sicherheitsrisiken einzugehen. Sie sollten zum Beispiel sichere Passwörter einsetzen und ihren Computer immer sperren, wenn Sie ihn verlassen. Es empfiehlt sich, sämtliche Sicherheitsupdates zeitnah einzuspielen, falls das nicht zentral von der Unternehmens-IT gesteuert wird. Wichtig ist außerdem, dass Sie keine Software nutzen, die von Ihrem Arbeitgeber nicht vorgesehen ist, zum Beispiel Cloudspeicher, Chatdienste oder Videokonferenzprogramme. Andernfalls entsteht eine Schatten-IT mit Risiken, die für die Unternehmens-IT schwer zu bekämpfen sind, weil sie sie gar nicht kennt. In unseren Security-Awareness-Seminaren, die wir für Kunden abhalten, steigen wir tiefer in diese Themen ein.

„Auch als User können Sie eine Reihe von Dingen tun, um unterwegs oder im Homeoffice keine unnötigen Sicherheitsrisiken einzugehen.“

Sie haben die Industrie 4.0 erwähnt – was sind hier die besonderen Herausforderungen und welche Lösungen bieten Sie konkret an?

Wenn Sie bedenken, dass Maschinen im Industrieumfeld oft länger als 30 Jahre in Betrieb sind, können Sie sich die Herausforderungen vorstellen: Eine digitalisierte und vernetzte Produktion ist extrem wichtig für zukunftsfähige Geschäftsmodelle, aber die Maschinen sind in vielen Fällen dafür schlichtweg zu alt. Wie bekommen die Betreiber diese Maschinen trotzdem sicher mit modernen Plattformen vernetzt? Mit secunet edge haben wir dafür eine Gesamtlösung im Portfolio, die auf dem Konzept des Edge Computing basiert: Die Lösung setzt dezentral an der einzelnen Maschine an, vernetzt sie und sichert sie ab. Darüber hinaus fungiert die Lösung als sichere Plattform, auf der diverse Connectivity-Anwendungen laufen können. So können die Betreiber zum Beispiel sichere Fernwartung umsetzen, mit einer Monitoring-Komponente Angriffe erkennen und vieles mehr. Dieses Konzept ist übrigens nicht nur für alte Maschinen, sondern auch für neue interessant: Es ist flexibel erweiterbar, sodass auch künftige Anforderungen abgedeckt werden können, die auch in neuen Maschinen – die wieder eine jahrzehntelange Laufzeit haben werden – noch nicht berücksichtigt sind.

Digitale Forensik ist ein neuer Fachbegriff, der in der Kriminalistik derzeit grassiert. Was versteht man darunter und welchen Beitrag leisten Sie als Unternehmen?

Digitale Forensik kommt dann zum Zug, wenn ein Cyberangriff erfolgreich war. Betroffenen Unternehmen bieten wir Forensik-Dienste an. Im Mittelpunkt steht dabei die Aufklärung des Sicherheitsvorfalls. Dessen Ursprung ist stets ein einzelnes kompromittiertes System, der sogenannte „Patient Zero“. Dieses System muss in vielen Fällen erst ermittelt werden. Dann erzeugen die Experten eine Eins-zu-eins-Kopie, um die Beweismittelkette zu erhalten, und analysieren anschließend die Kopie.

Zur digitalen Forensik gehört auch, als Unternehmen auf ein solches Szenario vorbereitet zu sein – das maximiert die Erfolgsaussichten im Ernstfall. Secunet bietet unter dem Stichwort „Forensic Readiness“ Workshops an, in denen Strukturen, Prozesse und Entscheidungsbäume festgelegt werden. Besonders wichtig sind ein gemeinsames Verständnis bei den beteiligten Personen sowie klare Rollen und Entscheidungskompetenzen.

Nehmen wir an, dass das Auto von morgen, die Straßenbahn, der Computer an der Arbeit, mein Smartphone, meine Bank, meine intelligente Brille etc. mit dem Internet verbunden sind. In diesem digitalisierten Umfeld, in das ich mich zunehmend mehr begebe, besteht die Gefahr einer digitalen Determination. Wie bewerten gerade Sie aus ethischer Sicht die Frage nach einer möglichen Einschränkung unserer Handlungsfreiheit durch die digitale Überhand?

Neue Technologien werden immer auch mit Skepsis betrachtet – das ist bei der digitalen Transformation, einer tiefgreifenden Umwälzung, natürlich nicht anders. Aber Sie sprechen durchaus eine Gefahr an, die wir ernst nehmen sollten.

Grundsätzlich gilt auch für die digitale Welt: Wir sind nur so unfrei, wie wir uns machen. Das fängt im Kleinen an: An Ihrem Smartphone sollten Sie bewusst und sorgfältig die Dienste auswählen, die Sie auch wirklich nutzen möchten, und die anderen deaktivieren. Im Großen spricht man von digitaler Souveränität. Sie ist ein Faktor, der der digitalen Determination entgegenwirkt. Digitale Souveränität bedeutet, die Hoheit über die eigenen Daten zu behalten – um sich vor Cyberkriminalität, Spionage und ähnlichem zu schützen, aber auch um in besonders sensiblen Bereichen unabhängig von den weltweit dominanten IT-Anbietern zu sein. Nur wer jederzeit weiß, wo seine Daten liegen und wer Zugriff darauf hat, kann auch entscheiden, was damit passiert. Das ist ein wichtiges Thema für Privatpersonen, aber auch für Unternehmen, Behörden und andere Organisationen. Bei secunet haben wir es uns daher zur Aufgabe gemacht, digitale Infrastrukturen zu schützen – weil wir unsere Kunden in die Lage versetzen wollen, digital souverän zu handeln und innovativ zu sein.

Ein Beispiel: Cloud Computing ist eine Technologie, die besonders stark mit dieser Frage verknüpft ist. Wir kennen das aus dem Privatleben: Wir nutzen Cloud-Angebote, weil sie praktisch sind. Aber wir haben manchmal ein schlechtes Gefühl dabei, weil wir nicht wissen, wo die Daten landen und ob sie nicht doch für Zwecke verwendet werden, die uns nicht gefallen. Für Behörden und Unternehmen, die mit besonders sensiblen Daten umgehen, haben wir dieses Dilemma mit secustack gelöst, einem Joint Venture von secunet und der Firma Cloud&Heat. SecuStack bietet ein vertrauenswürdiges Cloud-Betriebssystem – SecuStack – Made in Germany, basierend auf der Open Source Software „OpenStack“. Die Kernfunktion ist eine durchgängige Verschlüsselung der Daten in einer OpenStack-Umgebung mit den gleichen Sicherheitsbausteinen, die secunet seit vielen Jahren im Hochsicherheitsbereich einsetzt. Das ermöglicht es überhaupt, auf Basis prüfbarer Software eigene Cloud-Infrastrukturen für sensible Daten aufzubauen, so Cloud Computing zu nutzen und trotzdem souverän mit diesen Daten umzugehen.

Welche biometrischen Lösungen bietet Ihr Unternehmen an? Wie steht es um die Sicherheit meiner Daten, wenn ich mein Smartphone mit meinem Gesicht entsperre oder meine Bankzahlung via Fingerabdruck erledige?

Wir beschäftigen uns seit vielen Jahren intensiv mit Biometrie und ihrer Zuverlässigkeit und liefern zum Beispiel die Technologie, mit der an Flughäfen elektronische Reisepässe und Personalausweise automatisiert geprüft werden. Dabei nimmt das System ein Gesichtsbild der Reisenden auf und vergleicht es mit dem Bild auf ihrem elektronischen Identitätsdokument. Eine Vielzahl intelligenter Mechanismen sorgt dafür, dass Betrugsversuche keine Chance haben.

Die biometrischen Funktionen eines Smartphones sind auf jeden Fall ein besserer Schutz des Gerätes im Vergleich zu einer PIN oder gar keinem Zugriffsschutz. Die Bequemlichkeit der Nutzung ist zudem ein großer Vorteil, damit Anwender ihr Gerät überhaupt schützen. Allerdings sind die Mechanismen in den Smartphones weniger sicher gegen Angriffe als unsere Gesichtserkennung in den Grenzkontrollsystemen – denn bei diesen geht es ja auch um einen höheren Sicherheitsanspruch.

Was halten Sie von der Idee eines gänzlich digitalen Personalausweises?

Grundsätzlich spricht aus meiner Sicht nichts dagegen, ein digitales Abbild des Personalausweises für bequemere Identifikationsverfahren zu nutzen. Dieses sollte allerdings weiterhin an ein physisches Dokument gekoppelt sein, um bei Bedarf auch unabhängig von einer Smartphone-Funktion Identitätsprüfungen durchführen zu können.

Welche Rolle kann die enorme Leistungsfähigkeit eines Quantencomputers für die Datenverschlüsselung und andere kryptographische Verfahren spielen?

Der Quantencomputer ist eine große Chance für die effiziente Bearbeitung von Algorithmen, insbesondere im Kontext von Optimierungsfunktionen. Allerdings ist er gleichzeitig eine große Gefahr für herkömmliche Verschlüsselungsverfahren, da insbesondere für heutige asymmetrische Verfahren bereits Quantencomputer-Algorithmen existieren, die diese in sehr kurzer Zeit brechen. Aber es gibt durchaus Methoden, die sich quantenmechanische Effekte zunutze machen. Der Quantenschlüsselaustausch (QKD, Quantum Key Distribution) beruht auf quantenmechanischen Prozessen, die nachweislich sicher gegen Quantencomputer-Algorithmen sind.

Oder ist es umgekehrt: Kann gerade diese Leistungsfähigkeit eine neue Methode sein, um gängige Datenverschlüsselungssystem zu knacken?

Ja, für die herkömmliche Kryptographie sind Quantencomputer ganz klar eine Gefahr. Viele Verschlüsselungsverfahren basieren auf mathematischen Einwegfunktionen, die in eine Richtung leicht berechnet werden können, in die andere Richtung aber für heutige Computertechnik praktisch unmöglich zu berechnen sind. Quantencomputer werden aber künftig das bisher Unmögliche möglich machen. Daher sind Experten – auch bei secunet – seit einigen Jahren dabei, die Kryptographie gewissermaßen neu zu erfinden. Das Forschungsgebiet nennt sich Post-Quantum-Kryptographie. Wir sind dabei schon weit vorangekommen, es gibt bereits Quantencomputer-resistente Verschlüsselungsverfahren. Sie basieren auf anderen, komplexeren mathematischen Problemen als die herkömmlichen Methoden. Aktuell gilt es, diese Verfahren zu evaluieren und praxisbezogene Hindernisse aus dem Weg zu räumen.

Dazu beteiligen wir uns an internationalen Standardisierungsprozessen des National Institute of Standards and Technology (NIST) und der Internet Engineering Task Force (IETF), um frühzeitig unsere Produkte dafür zu ertüchtigen. Bereits im Jahr 2021 werden wir erste Produkte mit Post-Quantum-Kryptographie auf den Markt bringen.

Zuletzt ein Ausblick: Ist der Fortgang ins Digitale konstant steigend oder wird es auch wieder eine Renaissance des Analogen geben? Oder anders gefragt: Welche Bereiche unseres alltäglichen Lebens werden – aus Ihrer Sicht – von einer Digitalisierung verschont bleiben müssen, weil sie im Äther des Internets nicht funktionieren würden?

Aus meiner Sicht wird alles, was sich digitalisieren lässt, auch digitalisiert werden. Die digitale Welt bietet einfach zu viele Vorteile, um dieses Potenzial ungenutzt zu lassen. Als das papierlose Büro noch eine Zukunftsvision war, konnten sich viele nicht recht vorstellen, dass es einmal Realität werden würde. Heute zeigt nicht zuletzt die Corona-Krise, dass unzählige Homeoffice-Arbeitnehmer recht gut ohne Papierakten auskommen – und sie meist auch nicht vermissen.

Zudem entwickelt sich die Leistungsfähigkeit der Technologien unentwegt weiter bei tendenziell sinkenden Kosten – und der Automatisierungsgrad steigt stetig. Die viel beschworene „Künstliche Intelligenz“ ist z. B. nichts anderes als eine datenbasierte, automatisierte Programmierung – in diesem Fall von neuronalen Netzen. Damit scheint der Weg vorgezeichnet, dass digitale Systeme eine gewisse „Autonomie“ entwickeln und zu einer fortwährenden Digitalisierung drängen. Hier müssen wir aufpassen, dass wir immer die Kontrolle behalten, was da genau passiert – sozusagen digitale Souveränität 2.0.

Im privaten Bereich liegen die Dinge aktuell noch etwas anders: Schallplatten und gedruckte Bücher haben ihre Fans, weil Menschen mit diesen Medien positive Emotionen oder Erinnerungen verbinden. Allerdings gehört die Zukunft auch hier digitalen Formaten. Die analogen Inseln im digitalen Meer werden noch eine Weile Bestand haben, aber sicher nicht ewig.

Interview: Hannes Mittermaier

Dr. Kai Martius

Dr. Kai Martius ist seit 2015 CTO von secunet und wurde im Juni 2019 in den Vorstand berufen. Er verantwortet die Bereiche Technologie/Entwicklung, Produktmanagement und Zertifizierung. Zuvor leitete er von 2007 bis 2015 den Geschäftsbereich Hochsicherheit/Public Sector. Bereits seit 1999, dem Jahr seiner Promotion in der Elektrotechnik an der TU Dresden, war er bei secunet für verschiedene Themen in der Beratung und Produktentwicklung verantwortlich.

Dr. Martius zählt zu den maßgeblichen Architekten der Sicherheitslösung SINA und besitzt darüber hinaus umfangreiche Erfahrungen in der Konzeption, der Umsetzung und dem Einsatz von Sicherheitsprodukten im Behördenumfeld.

Fotos: secunet