SILICON SAXONY
MY FAVORITE PLACE

*11. SILICON **SAXONY** SYMPOSIUM 2013*

*MEGATREND **SICHERHEIT***

HERAUSFORDERUNGEN UND CHANCEN FÜR EINE VERNETZTE GESELLSCHAFT

www.silicon-saxony.de

Test and Integration Center

Das unabhängige und akkreditierte Software-Prüflabor.
Qualitätssicherung nach internationalen Standards für Ihre gesamte IT.

made in germany

Damit Hacker viele Hürden überwinden müssen, setzen Unternehmen typische Sicherheitslösungen wie Firewall und Virenschutz ein. Das ist unzureichend! Beste Voraussetzung für den Schutz Ihrer IT-Systeme: Eigene Schwachstellen und Bedrohungspotenziale kennen. Lassen Sie die Sicherheit Ihrer IT regelmäßig prüfen. Von zertifizierten Experten! IT-Security-Spezialisten, die die aktuellen Bedrohungsszenarien kennen und wissen, wie Hacker vorgehen. Minimieren Sie Ihr Risiko, das Opfer von Angriffen zu werden.

Beratung und Penetrationstests vom Web-Security-Spezialisten – dem Test and Integration Center von T-Systems Multimedia Solutions.
www.TIC-blog.de

13.00 **Begrüßung**
Heinz Martin Esser
(Vorstand Silicon Saxony e.V., Geschäftsführer Roth&Rau – Ortner GmbH)

13.05 **Grußwort**
Markus Ulbig
(Staatsminister des Sächsischen Innenministeriums)

1. SESSION: CYBERSECURITY UND BEDROHUNGEN AUS DEM INTERNET

Überblicksvorträge und Verortung des Themas Sicherheit aus unterschiedlichen Perspektiven

13.15 **Chancen und Risiken der globalen Vernetzung sowie Sicherheit in intelligenten Netzen**
Prof. Dr. Frank Schönefeld
(Geschäftsbereichsleiter Web Management Services, T-Systems MMS und Vorstandsmitglied im Silicon Saxony e.V., Dresden)

13.40 **Herausforderungen Cybersecurity für Staat, Wissenschaft und Wirtschaft**
Arne Schönbohm
(Vorstand BSS BuCET Shared Services AG und Präsident des Cyber-Sicherheitsrat Deutschland e.V., Berlin)

14:05 **Security in the Cloud – via Live-Hack kinderleicht sensible Unternehmens-daten manipulieren**
Thomas Haase
(Project Field Manager Data Privacy and Security, T-Systems MMS, Dresden)

2. SESSION: SICHERHEIT IN KRITISCHEN ANWENDUNGSBEREICHEN

Praxisbeispiele und Lösungsansätze aus verschiedenen Anwenderindustrien

14:30 **Tacho-Betrug – milliardenschwere Security-Herausforderung**
Arnulf Volkmar Thiemel
(Technischer Berater, Bereich Fahrzeugtechnik ADAC e.V., München)

14:55 **Innovationen für Sicherheit im Bereich Automotive**
Björn Steurich
(Senior Marketing Manager, Powertrain Systems Infineon Technologies AG, München)

15:20 **Funktionale Sicherheit im Kontext von Systemmanipulationen – Beispiele und Lösungsansätze aus der Praxis**
Marcus Rau
(Leiter, Competence Center Funktionale Sicherheit, SGS-TÜV Saar, Sulzbach)

15:45 - 16.00 **Kaffeepause – Get togehter**

3. SESSION: SICHERHEITSSTRATEGIEN FÜR EINE VERNETZTE GESELLSCHAFT

Bedrohungsszenarien und Abwehrstrategien im Kontext gesellschaftlich und wirtschaftlich kritischer Infrastrukturen

16:00 **Stuxnet – Cyberwar oder Industriespionage 2.0?**
Michael Hoos
(Technischer Direktor, Central EMEA Symantec GmbH, München)

16:25 **Sichere Programmierung – die Jagd nach dem Yeti**
Dr. Sebastian Broecker
(Chief Information Security Officer, DFS Deutsche Flugsicherung GmbH, Frankfurt am Main)

16:50 **Cyber-Sicherheit als strategische Herausforderung**
Prof. Dr. Holger Mey
(Head of Advanced Concepts, Cassadian, Unterschleißheim)

17:15 **„Military Grade Security" - Behörden- und Industrieanforderungen an IT-Sicherheit im Wandel der Zeit**
Dr. Kai Martius
(Head of Business Unit High Security, secunet Security Networks AG, Essen)

17:40 **Bedrohungen der Zukunft im militärischen Bereich**
Stéphane Beemelmans
(Staatssekretär im Bundesministerium für Verteidigung, zuständig für Administration und Ausrüstung, Berlin)

18:05 **Podiumsdiskussion:**

TEILNEHMER:

Stéphane Beemelmans
StS im Bundesverteidigungsministerium

Prof. Dr. Holger Mey
Cassidian

Michael Hoos
Symantec

Frank Schönefeld
T-Systems MMS

MODERATION:

Peter Carstens
Korrespondent Frankfurter Allgemeine Zeitung, Berlin, und Experte für Innen- und Verteidigungspolitik, Berlin

18:50 **Veranstaltungsende und Get togehter**

Das Internet ist aus dem Alltag der Menschen nicht mehr wegzudenken. Es ist ein umfassendes Instrument zur Information und Kommunikation. Es gibt kaum noch Geräte, die ohne Internetzugang auskommen – vom Smartphone über Tablets und Smart-TV bis hin zu Autos und sogar Kühlschränken.

Die zunehmende Vernetzung bietet den Menschen vor allem neue Möglichkeiten: Der Alltag wird durch intelligente Vernetzung und Steuerung des Haushalts effizienter und komfortabler. Über Smartphones und Tablets halten wir heutzutage mit dem mobilen Internet jederzeit den größten Wissensspeicher unseres Planeten in der Hand.

Auch die Staatsregierung sieht hier vor allem Chancen. Die E-Governmentstrategie des Freistaats bringt die Verwaltung mithilfe der neuen Technologien näher an den Bürger heran. Ziel ist, die meisten Behördengänge schnell und komfortabel von zu Hause aus erledigen zu können.

Klar ist aber auch: Sicherheit wird bei steigender Vernetzung der entscheidende Faktor für die Zuverlässigkeit solcher Systeme. Denn die neuen Möglichkeiten beinhalten auch Gefahren. Das fängt im privaten Bereich an: Daten werden abgegriffen oder ausspioniert, sei es beim Geldabheben am Automaten oder mittels falscher E-Mails im Internet. Schadprogramme und Trojaner werden gezielt von Verbrechern eingesetzt und digitale Identitäten werden gestohlen. Die Zahl der Betrugsfälle beim Online-Banking in Sachsen ist im letzten Jahr sprunghaft um 80 Prozent angestiegen.

Unsere Wirtschaft und unsere Infrastruktur funktionieren auf der Grundlage von vernetzten technischen Systemen. Spionage- und Hackerangriffe auf Unternehmen und Banken können somit zu einem ernsthaften volkswirtschaftlichen Problem werden. Vertreter der Bundesregierung gehen von einem Schadenspotenzial von bis zu 50 Milliarden Euro aus. Die Zahl von Angriffen wird in Zukunft zunehmen.

Was kann der Staat hier tun? Staatliche Aufgabe ist es zu allererst, die Menschen über diese Gefahren aufzuklären; Stichwort: Medienkompetenz. Denn Sicherheit fängt beim Wissen der Nutzer an.

Gleichzeit müssen die Sicherheits- und Strafverfolgungsbehörden auf der Höhe der Zeit arbeiten. Der Staat braucht genügend IT-Sachverstand, damit er potentiellen Angreifern mit Waffengleichheit begegnen kann. Außerdem brauchen wir klare gesetzliche Regelungen, die mit der technischen Entwicklung Schritt halten. Das Internet darf kein rechtsfreier Raum sein.

Allem voran muss der Staat die Sicherheit seiner eigenen IT-Infrastruktur gewährleisten. Das gilt insbesondere für die kritische Infrastruktur, wie bspw. bei Flughäfen oder Stadtwerken. Es gilt aber auch bei Fragen der Datensicherheit. Je mehr Verwaltungskommunikation über E-Government geschieht, desto mehr Daten geben die Bürger über digitale Kanäle preis. Aktuelle Trends wie bspw. Open Data und Cloud-Computing verstärken das Bedürfnis nach hohen und einheitlichen Standards bei Datenübermittlung und Datenverarbeitung. Hier sind zwei Dinge entscheidend: Nur gemeinsam erreichen wir ein hohes Sicherheitsniveau. Das bedeutet auch über die nationalstaatliche Ebene hinaus, Insellösungen sind in der vernetzten Welt der falsche Weg. Das komplexe Thema Cybersicherheit kann der Staat außerdem nicht alleine bewältigen – hier braucht es einen stetigen Dialog mit starken Partnern aus Industrie und Wissenschaft.

Um diesen Dialog zu fördern, hat das Sächsische Staatsministerium des Innern am 29. Oktober 2012 für seinen Geschäftsbereich einen Arbeitskreis Cybersicherheit als feste Institution etabliert. Der Arbeitskreis bewertet regelmäßig die aktuellen Entwicklungen auf dem Gebiet der Cybersicherheit und leistet damit einen aktiven Beitrag zu einer sicheren IT- Infrastruktur.

Ich freue mich sehr, dass auch das 11. Silicon Saxony Symposium dieses Thema aufgreift. Silicon Saxony steht für Innovation und Fortschritt. Ich bin mir sicher, dass die hier versammelten Experten aus Wirtschaft, Wissenschaft und Politik das Thema Cybersicherheit entscheidend voranbringen können. Allen Teilnehmern am Symposium wünsche ich daher viele neue Erkenntnisse, interessante Vorträge und spannende Diskussionen!

Markus Ulbig
Sächsischer Staatsminister des Innern

MEGATREND ***SICHERHEIT***

HERAUSFORDERUNGEN UND CHANCEN FÜR EINE VERNETZTE GESELLSCHAFT

In den letzten Wochen und Monaten war in den Medien wieder häufig von Datendiebstahl und Hackerangriffen auf Internetanbieter, Banken und Autos zu lesen – ein bedrohliches Szenario in der IT-Welt, das alle Bereiche im Spannungsfeld Gesellschaft, Umwelt, Ökonomie und Technologie umfasst. Hinter der Spionage-Malware Gauss etwa, sagt der russische Sicherheitsexperte Kaspersky Labs, steckten dieselben staatlich gestützten „Fabriken," die auch für Stuxnet, Duqu und Flame verantwortlich seien. Hacker 007 sozusagen – mit der Lizenz zum Hacken von Staats wegen?

SICHERE INFORMATIONS- UND KOMMUNIKATIONSTECHNOLOGIEN FÜR WIRTSCHAFT, POLITIK UND GESELLSCHAFT

Solche Netzattacken bezeichnet man als Cyberkriminalität. Und diese nimmt stetig zu. Das überrascht kaum: Wirtschaft, Politik und Gesellschaft sind heute mehr denn je auf Informations- und Kommunikationstechnologien (IKT) angewiesen – und das auf allen möglichen Endgeräten wie Handy, Smartphone, Tablet oder eBook mit allen damit zusammenhängenden Applikationen. Auf der einen Seite schaffen diese Technologien enorme Möglichkeiten für neues Wachstum und Beschäftigung. Auf der anderen Seite können unzureichende Sicherheitsvorkehrungen IKT-Systeme schnell zum Einfallstor für Wirtschaftssabotage und -spionage werden lassen. Schäden in Millionenhöhe drohen durch den Diebstahl von Daten und andere IT-Attacken.

SICHERHEIT ALS MEGATREND IN EINER VERNETZTEN WELT

Vor dem Hintergrund einer zunehmend vernetzten Welt und allen möglichen Angriffsszenarien auf IT-Systeme und IT-Netze entwickelt sich das Thema „Sicherheit" zum globalen Megatrend. Cyberattacken – wie auch immer motiviert und geartet – sind und bleiben eine große Herausforderung für Forschung, Wirtschaft und Politik. Denn die lebenswichtige Infrastruktur der internationalen Staatengemeinschaft hängt in immer größerem Maße von internettechnologiebasierten Netzwerken ab. Würden diese lahm gelegt oder manipuliert, käme das gesamte öffentliche Leben zum Stehen. Betroffen wären etwa das Transportwesen, die Versorgung mit Energie, Elektrizität und Wasser, das Gesundheitswesen, zivile Kommunikationssysteme sowie der Eisenbahn- und Flugverkehr. Mögliche Folgen: Satelliten trudeln aus ihrer Umlaufbahn, GPS-Systeme fallen aus, Navigationssysteme erblinden, Flugzeuge stürzen ab, Züge stoßen zusammen und Börsen und Banken müssen schließen. Auch die neue ‚Kommunikationsfähigkeit' von Autos birgt große Risiken – was, wenn Fahrassistenzsysteme durch Manipulation ungewollt zur Fernsteuerung werden?

INDUSTRIESPIONAGE BEREITS REALITÄT

Auch wenn Sicherheitsexperten die Sabotage kritischer, staatlicher Infrastrukturen – hier speziell der militärische Bereich – durch einen Cyberangriff aktuell als eher unwahrscheinlich einstufen, die Beispiele zeigen allemal, wie immens die Auswirkungen und die damit verbundenen Schäden im Ernstfall wären. Für die Wirtschaft hingegen ist das Ausspionieren von Industrie-Know-how bereits Realität. Unternehmen und Sicherheitsexperten weisen einhellig darauf hin, dass es durch das Manipulieren und Absaugen unternehmensrelevanter Daten zu globalen Wettbewerbsverzerrungen kommt. Ziel der Hacker sind dabei sensible Produktions- und Wirtschaftsdaten, aber auch Ausschreibungsinformationen: Erfährt die „Konkurrenz" Details zu Angeboten, Patenten oder anderen Formen geistigen Eigentums der Rivalen, kann von einem fairen Wettbewerb keine Rede mehr sein.

Je stärker Industrieprozesse oder sicherheitskritische Infrastrukturen vernetzt sind, desto höher ist das Risiko durch Cyberkriminalität.

ZUNEHMENDE VERNETZUNG ERFORDERT VIELSCHICHTIGE SICHERHEITSVORKEHRUNGEN

Alle Beispiele belegen eindrucksvoll, wie komplex, vielschichtig und interdependent das Thema „Sicherheit" heute ist. Dazu kommt eine relative Unklarheit, wie und in welchen Kontexten weitere Verwundbarkeiten und Lücken noch gedacht werden müssen. Zudem weiß kaum noch jemand, welche Sicherheitsmaßnahmen wo eingesetzt werden oder wie effektiv diese überhaupt sind. Die zunehmende Vernetzung sensibler Strukturen birgt Gefahren: Je stärker Industrieprozesse oder sicherheitskritische Infrastrukturen vernetzt sind, desto höher ist das Risiko durch Cyberkriminalität. Eine Antwort können alternative Kommunikationsnetze sein, nicht nur im militärischen Bereich, sondern auch z.B. im Gesundheitswesen, dem Banksektor und der Exekutive. Diverse Software, separate Systeme und auch verschiedene, voneinander getrennte Netzwerke reduzieren die Gefahren der Cyberkriminalität.

Dennoch bleibe das unangenehme Gefühl der Unsicherheit das wohl aktuell größte Problem im Zusammenhang mit der Cyberkriminalität. Die Industrie drängt zu schnellen und kostengünstigen Lösungen. Die Politik sieht sich mit neuen geostrategischen Fragestellungen konfrontiert, die Budgets für Forschung & Entwicklung, für Strategieplanung für ziviles Krisenmanagement und die Sicherung kritischer Infrastrukturen erfordern. Ein Beispiel ist die Task Force „IT-Sicherheit in der Wirtschaft" des Bundesministeriums für Wirtschaft und Technologie. Sie unterstützt kleine und mittelständische Unternehmen (KMU) bei der Verbesserung ihrer IT-Sicherheit.

SICHERHEIT ALS ZENTRALE HERAUSFORDERUNG FÜR DIE MIKRO- UND NANOELEKTRONIK

Für die Mikro- und Nanoelektronikbranche bedeuten Sicherheitsthemen in Bezug auf Elektronik aber noch eine weitere Herausforderung: Die Entwicklung, Produktion und der weltweite Vertrieb von Mikrochips, Software- und Hardware-Komponenten und elektronischen Geräten ist ihr Geschäft. Umso wichtiger ist es, dass diese den technologischen Anforderungen an Sicherheit nachhaltig gerecht werden, um auch zukünftig in einer zunehmend vernetzten Welt hochwertige und vor allem sichere Produkte auf den internationalen Markt liefern zu können.

Das Silicon Saxony Symposium greift diese Entwicklungen auf und bringt Referenten und Akteure aus unterschiedlichen Industrien und der Politik zusammen, die in diesem Spannungsfeld aktuelle Themen- und Handlungsfelder unter der thematischen Klammer „Sicherheit" von verschiedenen Perspektiven beleuchten. Sie diskutieren darüber hinaus die gegenwärtige Gefährdungslage und ihre möglichen Auswirkungen auf die Mikro- und Nanoelektronikbranche und geben auf dieser Basis Handlungsempfehlungen für KMUs. Das Thema des Symposiums verbindet insgesamt sowohl wirtschaftliche als auch technologische Gesichtspunkte, die für die Entwicklung der deutschen IKT-Industrie zwangsläufig eine bedeutende Rolle spielen. Die beiden Aspekte Betriebssicherheit (Safety) und Angriffssicherheit (Security) stehen dabei im Mittelpunkt der Diskussion.

PROF. DR. FRANK SCHÖNEFELD
Fachbereichsleiter „Software" im Silicon Saxony e.V. und Prokurist bei T-Systems MMS

CYBERSECURITY UND BEDROHUNGEN AUS DEM INTERNET

ÜBERBLICKSVORTRÄGE UND VERORTUNG DES THEMAS SICHERHEIT AUS UNTERSCHIEDLICHEN PERSPEKTIVEN

Beginnend mit den Arbeiten zum Arpanet zur Vernetzung von Computern Ende der 60er Jahre hat ein mittlerweile 40 Jahre andauernder Innovationszyklus begonnen, der in der Herausbildung des Internets in den 80er Jahren und des World Wide Webs in den 90er Jahren kulminierte.

Heute nutzen über 2,3 Milliarden Menschen das Internet, davon allein ca. 1 Milliarde mit Zugängen über mobile Geräte (Smartphones, Tablets). Der Datenverkehr über das Netz der Netze hat mittlerweile ein Volumen von über 400 Exabyte pro Jahr erreicht.

Während die ersten „Hacker" noch einzelne Computer auseinander- und umbauten, um deren Leistung zu steigern, führte die Vernetzung von Computern auch zu einer völlig neuen Dimension bzgl. der Erreichbarkeit von Angriffszielen. Der „ILoveyou"-Wurm im Jahr 2000 infizierte ca. 20% aller mit dem Internet vernetzten Computer. Mit der Nutzung des World Wide Web als Transaktionsmedium (Abwicklung geschäftlicher Aktivitäten, E-Commerce, Online Banking) steigerte sich die „Attraktivität" des Netzes und seiner Computer für Angreifer erheblich, da tatsächliche monetäre Bewegungen ausgelöst werden können.

Ein möglicher neuer Innovationszyklus der Weltwirtschaft könnte mit dem Übergang zu sogenannten intelligenten Netzen beginnen. Darunter versteht man Energieinformationsnetze, Smart City Infrastrukturen (u.a. Verkehrsinfrastruktur), moderne Gesundheitsnetze, Bildungsnetze und Behördennetze. Insbesondere bei den Energieinformationsnetzen und den Smart City Infrastrukturen kommen neben den Sensoren zur Erfassung der Realzeit-Situation, Aktoren zur aktiven Beeinflussung der Situation (Verkehrsflusssteuerung, virtuelle Kraftwerkssteuerung aus 100.000 Haushalten) zum Tragen – cyber-physikalische Systeme entstehen. Techniken und Technologien des Internet und des World Wide Web werden wichtige Bestandteile dieser intelligenten Netze darstellen.

Unter diesen Vorzeichen verstärkt sich die Dramatik möglicher Cyberangriffe erheblich – kritische Infrastrukturen einer Volkswirtschaft und Gesellschaft geraten in das Fadenkreuz potentieller Angreifer, die längst den Hackerkinderschuhen entwachsen sind und eher als strategisches Potential einer neuen Art der Destabilisierung verstanden werden. Folgerichtig weist die Wachstumsrate an Cyberkriminalität seit Jahren zweistellige Werte aus.

Für die handelnden Akteure (Wirtschaft, Politik) einer Volkswirtschaft und Gesellschaft bedeutet dies eine erhebliche Verantwortung für die richtige Einschätzung dieser Entwicklungen sowie ein strategisch und wirtschaftlich sinnvolles Umgehen mit den potentiellen Gefahren. Dazu gehört insbesondere das Betrachten von Sicherheitsaspekten der gesamten Kette cyberphysikalischer Systeme – beginnend von Mikrosystemen hin zu Software bis zu den Protokollen der Netzsteuerung und nicht zu vergessen – der menschliche Faktor.

Die Vorteile einer umfassenden Vernetzung einer Volkswirtschaft sind derart überzeugend, dass sie schlechthin als unverzichtbar gelten muss. Der neuen Dimension in der Bedrohung durch Cyberangriffe sollte ebenfalls mit einer neuen Dimension an Sicherheitskonzepten und – umsetzungen entgegen getreten werden. Die Lehren aus 20 Jahren Internet und WWW liegen vor.

UWE GÄBLER
Fachbereichsleiter „Applikationen“
im Silicon Saxony e.V.,
Infineon Technologies Dresden GmbH

SICHERHEIT IN KRITISCHEN ANWENDUNGSBEREICHEN

PRAXISBEISPIELE UND LÖSUNGSANSÄTZE AUS VERSCHIEDENEN ANWENDERINDUSTRIEN

Sicherheit ist zu einem essentiellen gesellschaftlichen Bedürfnis geworden – entscheidend für Vertrauen, Schutz und Privatsphäre. Der Sicherheitstrend kristallisierte sich zunächst in den Bereichen Telekommunikation, Finanztransaktionen, hoheitliche Ausweisdokumente und Trusted Computing heraus. Die Bereiche Automobil- und Industrieanwendungssysteme sehen nun auch einen ähnlichen Bedarf, sich vor Risiken zu schützen. Seitens der Automobilhersteller wächst hierbei unter anderem der Wunsch nach einem höheren Manipulations- und Tuningschutz ihrer Fahrzeuge.

Die Entwicklung der modernen Informations- und Kommunikationstechnologie – Gesellschaft basiert in hohem Maße auf der Verfügbarkeit elektronischer Daten und einer Vielzahl vernetzter Geräte: IT-Dienstleistungen, wie zum Beispiel Cloud Computing oder kritische Infrastruktureinrichtungen wie zum Beispiel das intelligente Stromnetz (Smart Grid). Die oft sehr schützenswerten Daten sollen weder manipuliert noch gestohlen werden können. Chips, zum Beispiel auf Basis der digitalen Sicherheitstechnologie „Integrity Guard“ von Infineon, helfen solche Anwendungen abzusichern. Aber es muss nicht immer ein separater Chip sein. Hardware-basierte Sicherheit wird zunehmend ein wichtiger funktionaler Bestandteil anderer Komponenten. So wird beispielsweise ein Hardware-Security-Modul (HSM) in Infineons neuester Familie von 32-bit-Multi-Core-Mikrocontrollern (AURIX) für Automobilanwendungen für den verbesserten Schutz vor Manipulation sowie gegen das unerlaubte Auslesen der Daten und Programme eingesetzt. Die Industrie steht hier erst am Anfang einer Entwicklung.

Dies wird sehr deutlich, wenn man beispielsweise das Thema Tacho-Betrug betrachtet. Der Kilometerstand in fast allen aktuellen Autos kann sehr einfach und schnell manipuliert werden. Nach Ermittlungen der Polizei werden jedes Jahr rund zwei Millionen Gebrauchtwagen allein in Deutschland manipuliert. Pro Fahrzeug entsteht im Schnitt ein Schaden von 3.000 Euro. Das bedeutet einen Gesamtschaden von rund sechs Milliarden Euro pro Jahr - fast ausschließlich zu Lasten der Gebrauchtwagenkäufer. Herr Thieme vom ADAC berichtet im Rahmen seines Vortrags von der „Initiative gegen Tacho-Betrug“ und der Forderung des ADAC nach gesetzlichen Vorschriften zum zeitgemäßen Schutz gegen Tacho-Betrug.
Nach einer Übersicht über die beobachteten IT- Angriffe im Fahrzeug, greift Herr Steurich (Infineon Technologies AG) das Thema Tacho-Betrug auf und stellt einen Lösungsansatz basierend auf den AURIX Mikrocontrollern vor. Eine Kernaussage ist hierbei, dass die Aspekte der funktionalen Sicherheit und der Datensicherheit im Fahrzeug nicht unabhängig voneinander betrachtet werden dürfen.

Abgerundet wird dieser Vortragsteil von Herrn Rau (SGS-TÜV Saar GmbH), der über funktionale Sicherheit im Kontext von System-Manipulationen spricht. Er liefert dazu Beispiele und Lösungsansätze aus der Praxis.

HEINZ MARTIN ESSER
Vorstand im Silicon Saxony e.V. und
Geschäftsführer Roth & Rau - Ortner GmbH

3. SESSION

SICHERHEITSSTRATEGIEN FÜR EINE VERNETZTE GESELLSCHAFT

BEDROHUNGSSZENARIEN UND ABWEHRSTRATEGIEN IM KONTEXT GESELLSCHAFTLICH UND WIRTSCHAFTLICH KRITISCHER INFRASTRUKTUREN

Cyberkriminalität hat viele Facetten und betrifft alle Mitglieder der Gesellschaft: Privatpersonen, die z.B. elektronisch ihre Bankgeschäfte erledigen, Unternehmen, die im globalen Wettbewerb ihr Know-how und Geschäftsdaten sichern, Kommunen, Städte und Länder, deren Infrastrukturen sich zunehmend vernetzen, und auch Nationalstaaten, die Sektoren des öffentlichen Lebens – wie Verkehr und Energieversorgung – aber auch Militärstrukturen schützen müssen.

Die vorangegangenen Sessions beschäftigten sich mit der Sicherheit moderner Informations- und Kommunikationstechnologie – und meinten damit die Softwareseite. In der abschließenden Session werfen die Teilnehmer nun einen Blick auf die Hardwarekomponente: Mikro- und Nanoelektronik, die Chips, Sensoren und Übertragungsmodule, das ist das Herz der vernetzten Gesellschaft. Sie bildet die Grundlage für Informations- und Kommunikationstechnologie und ist damit eine Schlüsseltechnologie für Produkte und Dienstleistungen in einer vernetzten Welt.

Darum müssen wir uns fragen: Was nützt die sicherste Software, die durchdachteste Datenstruktur, wenn die Hardware, auf der sie installiert ist, selbst ein Einfallstor für Cyberattacken darstellt? Wenn Chips und Sensoren in Asien produziert werden und quasi werkseitig bereits so konfiguriert sein können, regelmäßig „nach Hause zu funken"? Wie sicher können moderne militärische Systeme, Firmendaten, Kraftwerke und Verkehrsleitsysteme sein, wenn sie auf Steuerungselementen aus potentiell unsicheren Produktionsstätten beruhen?

Europa ist stark in der Mikro- und Nanoelektronik. Hier gibt es eine einzigartige Ballung von Industrieunternehmen und Forschungseinrichtungen, die mit ihrer Arbeit in der Vergangenheit die Grundlagen für eine sichere Informations- und Kommunikationstechnologie gelegt haben und weiterhin Technologietreiber sein werden. Die Produktion der Technologie und die Forschungs- und Entwicklungskompetenz wandert jedoch zusehends ab – und mit ihr die Kontrolle über wirklich sichere IT. Diese Entwicklung betrifft nicht nur die Mikroelektronikbranche – auch die europäische Automobilindustrie, der Maschinenbau und die Luft- und Raumfahrtbranche sind auf Produktinnovationen auf Basis der Mikroelektronik angewiesen. Vor diesem Hintergrund sind verlässliche Strategien für die Prüfung und Zertifizierung von Halbleiterprodukten unumgänglich.

Um den zukünftigen Sicherheitsherausforderungen gewachsen zu sein, braucht es eine weiterhin starke europäische Mikroelektronik. Dafür sind wir auch auf die Unterstützung der europäischen Politik angewiesen.

*SILICON **SAXONY***

SÄCHSISCHES HOCHTECHNOLOGIE-CLUSTER

Der Freistaat Sachsen gehört zur internationalen Spitze. Silicon Saxony, die Region zwischen Freiberg, Chemnitz und Dresden, ist Europas größter Mikroelektronikstandort. Hier erforschen, entwickeln und produzieren Unternehmen und Forschungseinrichtungen moderne Informations- und Kommunikationstechnologie (IKT). Das sächsische Hochtechnologie-Cluster vereint Know-how in den Bereichen Mikro- und Nanoelektronik, Telekommunikationstechnologie, Photovoltaik, IT und Informationstechnik, energieeffiziente Systeme, Smart Systems und vernetzte Sensorik sowie organische und gedruckte Elektronik.

Etwa 2.100 sächsische Unternehmen mit insgesamt 51.000 Mitarbeitern sind auf allen Stufen der IKT-Wertschöpfungskette aktiv: Sie entwickeln, fertigen und vermarkten integrierte Schaltkreise oder dienen der Chipindustrie als Material- und Equipmentlieferanten, produzieren und vertreiben elektronische Produkte und Systeme auf der Basis integrierter Schaltungen oder entwickeln und vermarkten Software. Gemeinsam setzen sie jährlich gut acht Milliarden Euro um.

Die hauptsächlich kleinen und mittelständischen Unternehmen profitieren vom starken akademischen Umfeld im Freistaat: 10 Fraunhofer-Institute, 5 industrielle Forschungsinstitute und 1 Max-Planck-Institut forschen an Hochtechnologien und 7 Bildungseinrichtungen bilden die Experten von morgen aus.

Der Silicon Saxony e.V. vereint über 300 Mitgliedsunternehmen, die einen Umsatz von mehr als 4,5 Milliarden Euro pro Jahr erzielen. Damit ist das Branchennetzwerk für Mikro- und Nanoelektronik, Photovoltaik, Software, Smart Systems und Applikationen das größte in Europa. In Arbeitskreisen entwickeln seine Mitglieder Innovationen und profitieren dabei vom vorhandenen Technologiespektrum am Standort. Sie arbeiten z.B. an cyber-physikalischen Systemen – auf Basis hochqualitativer Mikroelektronik und Software.

*SILICON **SAXONY** e.V.*
Manfred-von-Ardenne-Ring 20
01099 Dresden
Telefon +49 (351) 8925-888
Fax +49 (351) 8925-889
info@silicon-saxony.de
www.silicon-saxony.de

SETZEN SIE AUF GELB.

So beantwortet Symantec™ Ihre Fragen rund um den Schutz von Informationen.

DATA LOSS PREVENTED

CLOUDS SECURED

ENDPOINTS PROTECTED

MOBILE DEVICES SECURED

INFORMATION PROTECTED

SECURITY ASSURED

Weitere Informationen finden Sie unter:
www.symantec.de

Symantec™