Fraunhofer SIT

FRAUNHOFER-INSTITUT FÜR
SICHERE INFORMATIONSTECHNOLOGIE

# Security Mythen

## » Sicherheitsvorkehrungen sind unnötig, die Hacker knacken doch sowieso alles. «

Mit dieser Einstellung könnten Sie genauso gut Ihre Haustüre sperrangelweit offen stehen lassen. Schließlich bietet auch ein Türschloss nicht den ultimativen Einbrecherschutz. Dennoch schließt jeder seine Haustüre ab – und das ist auch gut so. Denn sowohl in der realen als auch in der virtuellen Welt schaffen Sie so Hürden für Einbrecher. Viele der aktuellen Angriffe lassen sich bereits mit Standard-Sicherheitsvorkehrungen abwehren, nur werden diese in vielen Unternehmen noch nicht oder nicht richtig umgesetzt.

Übrigens, wenn Sie sich mittels Verschlüsselung absichern, kommt dies einem nahezu unknackbaren Tresor gleich, denn selbst Nachrichtendienste können gute Verschlüsselungen praktisch nicht knacken.

Fraunhofer SIT

Fraunhofer-Institut für Sichere Informationstechnologie
Rheinstraße 75 · 64295 Darmstadt
www.sit.fraunhofer.de


superkali
fragilistis
chexpiali
getisch

# » Je länger das Passwort, desto sicherer. «

Hand aufs Herz: Passwörter sind irgendwie nervig. Für jede Anwendung soll man sich ein Eigenes ausdenken. Wer soll sich das alles merken? Da ist es doch einfacher, ein richtig langes Passwort zu verwenden.

Nicht so ganz: Viele verwenden bei langen Passwörtern Wörter aus dem Wörterbuch. Doch selbst 20-stellige Passwörter aus dem Wörterbuch sind oft leichter zu knacken als kürzere mit Sonderzeichen.

Für ein sicheres Passwort nehmen Sie beispielsweise die Anfangsbuchstaben eines Satzes, den Sie sich gut merken können. Achten Sie dabei auch auf die Groß- und Kleinschreibung der Wörter und bauen Sie Zahlen oder Sonderzeichen ein.

Beispiel: Hans kauft sich jeden Tag 1 Apfel! --> **HksjT1A!**

Fraunhofer SIT

Fraunhofer-Institut für Sichere Informationstechnologie
Rheinstraße 75 · 64295 Darmstadt
www.sit.fraunhofer.de

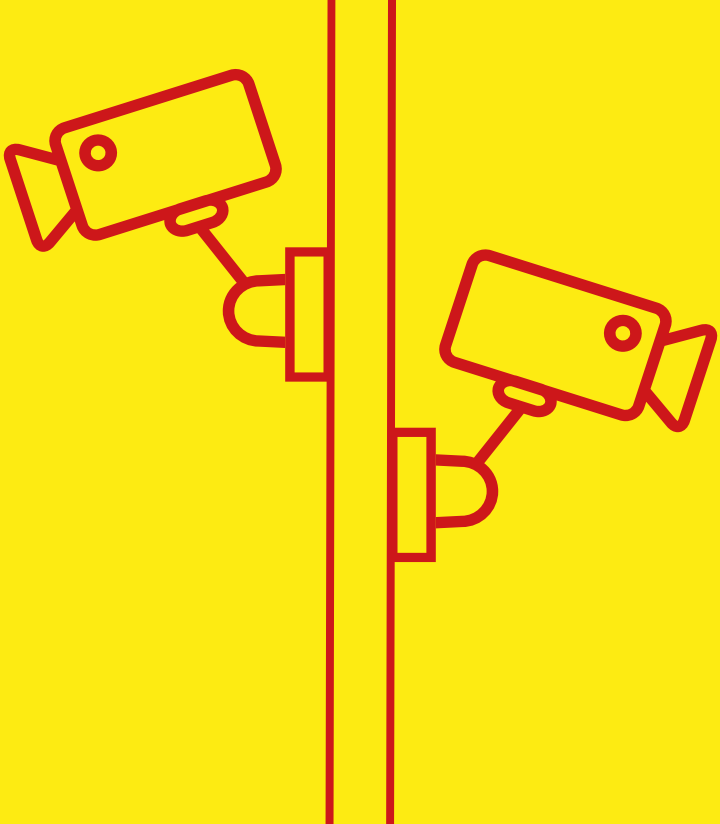
## » Wenn ich ein gutes Passwort habe, dann kann keiner meine E-Mails lesen. «

Leider ist das nicht ganz richtig. Unverschlüsselte E-Mails passieren auf ihrem Weg vom Sender zum Empfänger zahlreiche Stellen, an denen Angreifer die Inhalte abfangen und lesen können: Schreiben Sie beispielsweise Ihre E-Mail von einem offenen WLAN eines Cafés aus, ist der Zugriff ein Leichtes für Hacker. Auch beim E-Mail-Provider oder Internet-Service-Provider kommen die Mails auf dem Weg zum Empfänger vorbei und können leicht abgefangen werden. Übrigens, auch die Administratoren Ihres Unternehmens können unverschlüsselte E-Mails mitlesen.

Abhilfe schafft hier nur eine gute Verschlüsselung, wie sie beispielsweise die Volksverschlüsselung anbietet. Mit der Ende-zu-Ende-Verschlüsselung der Nachricht wird sichergestellt, dass nur Sender und Empfänger Nachrichten im Klartext lesen können.

Fraunhofer SIT

Fraunhofer-Institut für Sichere Informationstechnologie
Rheinstraße 75 · 64295 Darmstadt
www.sit.fraunhofer.de



## » Ich muss nicht verschlüsseln, ich habe nichts zu verbergen. «

Auch wer nichts zu verbergen hat, sollte darauf achten, wie und was er kommuniziert. Cyberkriminelle nutzen alle verfügbaren Daten, die sie finden, für ihre Zwecke. Sie spähen Sie aus und können anhand unverschlüsselter Nachrichten an Kontodaten oder Zugänge zu verschiedenen Portalen, wie Amazon, gelangen. Mit den Funktionen »Passwort vergessen« und »Passwort ändern« können die Kriminellen Ihre Konten übernehmen, Ihre Identität stehlen und Sie sogar ungewollt in kriminelle Machenschaften hineinziehen.

Eine gute Verschlüsselung beugt also nicht nur unerlaubter Massenüberwachung vor, sondern schützt auch vor Identitätsdiebstahl.

Fraunhofer SIT

Fraunhofer-Institut für Sichere Informationstechnologie
Rheinstraße 75 · 64295 Darmstadt
www.sit.fraunhofer.de

Es war
einmal ...

# » Gute Verschlüsselung ist viel zu kompliziert. «

Im vergangenen Jahr hatten nur 15 Prozent der deutschen Internetnutzer eine Software für die E-Mail-Verschlüsselung installiert. So das Ergebnis einer repräsentativen Befragung, die der Industrieverband Bitkom Anfang 2016 durchführte. Der Grund, warum nicht mehr Menschen verschlüsselt kommunizieren ist, dass die Einrichtung einer wirksamen Verschlüsselung für viele zu schwierig ist.

Dabei muss Verschlüsselung nicht immer kompliziert sein. WhatsApp machte es für den Messenger-Dienst vor. Die Nutzer hatten keinen Aufwand und können seither abhörsicher kommunizieren. Für die E-Mail-Kommunikation hat das Fraunhofer SIT die laientaugliche Volksverschlüsselungs-Software entwickelt. Mit ihr können E-Mails mit wenigen Klicks Ende-zu-Ende verschlüsselt werden.

Fraunhofer SIT

Fraunhofer-Institut für Sichere Informationstechnologie
Rheinstraße 75 · 64295 Darmstadt
www.sit.fraunhofer.de

# » IT-Sicherheit und Datenschutz sind ein notwendiges Übel. «

Die vernetzte Industrie 4.0 ist auf dem Vormarsch, selbstfahrende Autos kurven bereits durch unsere Straßen und nahezu jeder hat schon einmal etwas online bestellt. Erst mit ausreichend IT-Sicherheit und Datenschutz wird dies alles möglich, denn erst die Schutzmaßahmen sorgen bei den Nutzern für Vertrauen in die neue Technik.

Nicht auszumalen, was passieren könnte, wenn ein Angreifer die Kontrolle über ein vernetztes Fahrzeug übernimmt oder bei Amazon Ihre Kontodaten klaut. IT-Sicherheitsfunktionen verhindern dies. Ähnliches gilt für den Datenschutz: Nicht jeder Autobesitzer möchte, dass alle vom Auto gesammelten Daten haarklein an Hersteller oder Versicherung gehen.

Wie man sieht, betreffen IT-Sicherheit und Datenschutz jeden. Sie sind kein notwendiges Übel, sondern schützen vor Schaden und stellen einen aktiven Verbraucherschutz dar.

Fraunhofer SIT

Fraunhofer-Institut für Sichere Informationstechnologie
Rheinstraße 75 · 64295 Darmstadt
www.sit.fraunhofer.de

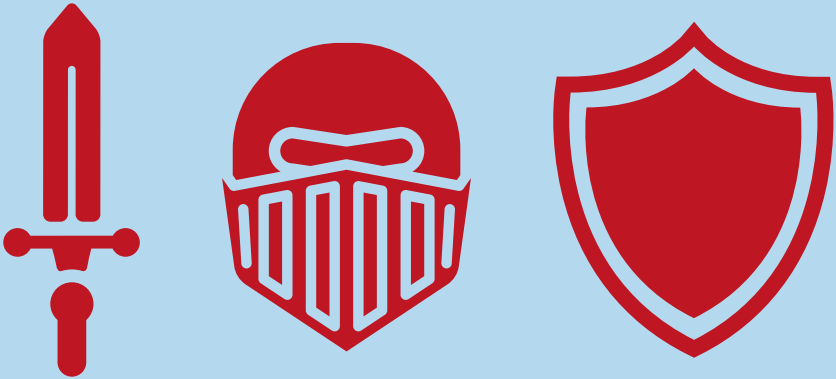
## » Ich habe Sicherheitssoftware installiert, damit passiert mir nichts. «

Vertrauen Sie nicht blind auf einen Schutzmechanismus, denn mit den IT-Sicherheitsvorkehrungen verhält es sich oft wie mit den Sicherheitsfunktionen im Auto: Wenn Ihnen bei 150 km/h auf der Autobahn ein Reifen platzt oder Ihnen an einer Kreuzung jemand die Vorfahrt nimmt, lässt sich ein Unfall oft nicht vermeiden. Sicherheitsanwendungen helfen nur gegen bestimmte oder bekannte Bedrohungen. Gegen neuartige Gefahren und unvorhergesehene Situationen können sie nur schwer etwas ausrichten.

Daher gilt: Schützen Sie sich so gut wie möglich, aber surfen Sie auch vorausschauend durch das Internet und vermeiden Sie unnötige Risiken.

Fraunhofer SIT

Fraunhofer-Institut für Sichere Informationstechnologie
Rheinstraße 75 · 64295 Darmstadt
www.sit.fraunhofer.de



## » Je mehr Sicherheitsmaßnahmen, desto sicherer wird mein System. «

Nicht alleine die Anzahl der Maßnahmen, sondern auch die Umsetzung der Sicherheitsvorkehrungen ist entscheidend: Eine dicke Ritterrüstung bringt Ihnen nichts, wenn Sie sich mit ihr nicht mehr bewegen können und angreifbar werden.

Je komplexer ein System wird, desto schwieriger ist es zu kontrollieren: Sicherheitsmaßnahmen können sich gegenseitig angreifen oder außer Kraft setzen, und selbst Sicherheitssysteme können Schwachstellen besitzen, die Angreifer ausnutzen können.

Bevor Sie also eine Vielzahl an Sicherheitsvorkehrungen ergreifen, überlegen Sie sich zuerst, was Sie schützen wollen und dann mit welchen Maßnahmen dies am besten gelingt. So senken Sie vermutlich die Kosten und erhöhen gleichzeitig den Nutzen.

Fraunhofer SIT

Fraunhofer-Institut für Sichere Informationstechnologie
Rheinstraße 75 · 64295 Darmstadt
www.sit.fraunhofer.de

## » Geheime Sicherheitsverfahren sind immer sicherer als öffentlich bekannte Algorithmen. «

Diese Aussage ist mit Vorsicht zu genießen: Der Bekanntheitsgrad eines Verfahrens sagt zwar nichts über dessen Sicherheit aus, aber in der Regel sind öffentliche Algorithmen sicherer als geheime Verfahren. Bei öffentlich zugänglichen Sicherheitsverfahren haben alle die Möglichkeit, sie nachzuvollziehen und zu prüfen, und viele Wissenschaftler tun das auch. Wenn ein Verfahren von vielen Menschen geprüft wurde, ohne dass Fehler gefunden wurden, gilt es als sicher. Hier gilt: Mehr Augen entdecken mehr Schwachstellen und mehr Köpfe können zusammen bessere Lösungen entwickeln.

Zudem beruhen viele Sicherheitsalgorithmen auf mathematischen Problemen, an denen sich Mathematiker seit Jahrhunderten die Zähne ausbeißen.

Fraunhofer SIT

Fraunhofer-Institut für Sichere Informationstechnologie
Rheinstraße 75 · 64295 Darmstadt
www.sit.fraunhofer.de

# ENE MENE MUH

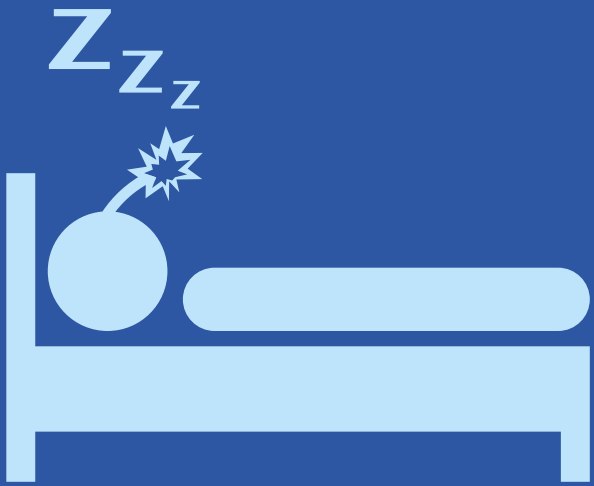
## » Ich habe nichts Wichtiges auf meinem Rechner. Mein Computer ist deshalb kein Angriffsziel. «

Sie denken vielleicht Ihr Rechner sei für Cyberkriminelle uninteressant. Doch Angreifer sehen das oft anders, denn nicht immer sind ausgespähte (Konto-) Daten oder Identitätsdiebstahl Ziel der Hacker. Manchmal geht es denen einfach um Erpressung. Dazu werden einfach alle Dateien auf Ihrem Rechner verschlüsselt und erst gegen Zahlung eines Lösegeldes – vielleicht – freigegeben. In vielen Fällen richtet sich der Angriff auch gar nicht direkt gegen Sie als Besitzer des Rechners, sondern Ihr Rechner wird als Bot für Cyberangriffe auf Unternehmen benötigt. Mit Hilfe von sogenannten Bot-Netzen können Angreifer etwa viele Bot-Rechner zu einer riesigen Angriffsmaschine zusammenschließen und großen Schaden anrichten.

Übrigens richtet sich die Anfälligkeit für automatisierte Massenangriffe nach dem Schutzniveau Ihres Computers. Sprich: Ist der eigene Rechner anfällig, wird er irgendwann auch angegriffen.

Fraunhofer SIT

Fraunhofer-Institut für Sichere Informationstechnologie
Rheinstraße 75 · 64295 Darmstadt
www.sit.fraunhofer.de


Z
Z
Z

## » Wenn der eigene Rechner infiziert ist, merkt man das. «

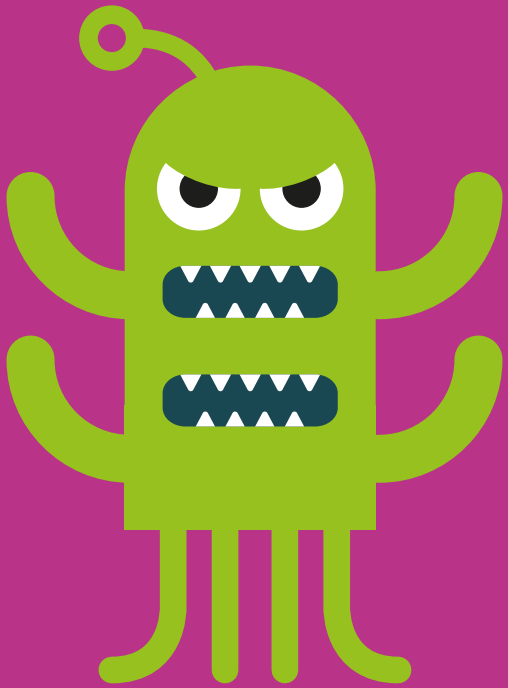
Sie wachen morgens mit einer Erkältung auf, dabei war gestern noch alles in Ordnung. Doch die Viren schlummerten bereits seit Tagen in Ihrem Körper, ohne dass Sie es bemerkt haben.

Mit Schadsoftware verhält es sich häufig genauso – sie schläft längere Zeit unbemerkt, bis der Angreifer sie aktiviert. Die Cyberkriminellen haben dabei beispielsweise das Ziel den Nutzer auszuspähen und so Zugangsdaten oder Konto- und Kreditkartennummern auszuspionieren. Damit können sie den Opfern einen erheblichen wirtschaftlichen Schaden zufügen.

Auch wenn es keinen absolut sicheren Schutz gibt, sollten Sie daher immer Ihre Antivirenprogramme und Firewalls aktuell halten und bereitgestellte Sicherheitsupdates installieren.

Fraunhofer SIT

Fraunhofer-Institut für Sichere Informationstechnologie
Rheinstraße 75 · 64295 Darmstadt
www.sit.fraunhofer.de



## » Ich surfe nicht auf Pornoseiten, deshalb kann ich mir nichts einfangen. «

Laut einer Studie von Gdata machen Porno-Seiten nur rund fünf Prozent der bösartigen Websites aus. Allgemeine Wirtschafts-, Technik-, Gesundheits- und Kommunikationsseiten sowie Blogs stellen eine viel größere Gefahr dar. Mitunter haben seriöse Online-Shops ungeliebte Untermieter, also Seiten, die andere und zum Teil illegale Dinge zum Kauf anbieten. Schadsoftware versteckt sich auch gerne in Werbebannern und kann sich beim Anklicken unbemerkt auf Ihrem PC installieren.

Auch wenn sie nicht unfehlbar sind, ein gründlicher Schutz durch Antivirenprogramme und Firewalls sowie regelmäßige Sicherheitsupdates sind auf jeden Fall empfehlenswert.

Fraunhofer SIT

Fraunhofer-Institut für Sichere Informationstechnologie
Rheinstraße 75 · 64295 Darmstadt
www.sit.fraunhofer.de

## » Ich öffne nur Mails von Freunden und Bekannten, deshalb kann mir nichts passieren. «

Der Wolf im Schafspelz ist nicht immer auf den ersten Blick zu erkennen – das gilt für viele Bereiche. Absenderadressen zu fälschen, ist für Cyberkriminelle ein Kinderspiel. Die E-Mail-Fälschung ist immer noch ein beliebtes Mittel, da sich so immer noch viele Angriffe erfolgreich durchführen lassen. Oft sehen die E-Mails täuschend echt aus und können Sie, wie der Wolf im Märchen, in die Falle locken.

Seien Sie deshalb auch bei E-Mails von Bekannten und Freunden vorsichtig, wenn diese Sie bitten, einem Link zu folgen oder einen Anhang zu öffnen. Eine kurze Rückfrage kann Ihnen viel Ärger ersparen.

Fraunhofer SIT

Fraunhofer-Institut für Sichere Informationstechnologie
Rheinstraße 75 · 64295 Darmstadt
www.sit.fraunhofer.de


20
Oktober

## » Passwort-Aktualisierungen erhöhen stets die Sicherheit. «

Und täglich grüßt das Murmeltier: Kennen Sie das auch? Der neue Monat hat angefangen und Ihr Rechner fordert Sie auf, sich ein neues Passwort zu überlegen. Dabei waren Sie gerade froh, sich das alte Passwort merken zu können. Die Folge von sehr häufigen Passwort-Aktualisierungen ist, dass Nutzer dazu neigen einfache Passwörter zu wählen, die leichter geknackt werden können. Oder sie schreiben sich das neue Passwort auf und kleben es an den PC. So kann jeder auf den Rechner zugreifen.

Passwörter sollen regelmäßig, aber nicht zu häufig aktualisiert werden. Wichtig ist zudem, dass Sie für verschiedene Dienste auch unterschiedliche Passwörter verwenden. Wer sich dennoch seine Passwörter nicht merken kann, sollte seriöse Software zur Passwortverwaltung nutzen.

Fraunhofer SIT

Fraunhofer-Institut für Sichere Informationstechnologie
Rheinstraße 75 · 64295 Darmstadt
www.sit.fraunhofer.de


0
0
1
0
1
1
0
1
0
1
0
1
0
1
0
1
0
1
0

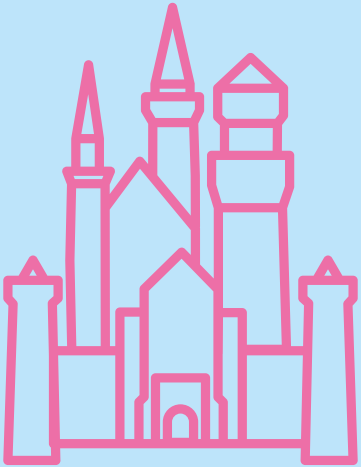
# » In der Cloud ist alles unsicher. «

Wie sicher die Daten sind, hängt von der konkreten Umsetzung der Cloud-Lösung ab. Die grundsätzlichen Fragestellungen hierzu hat das Fraunhofer SIT hat in seiner Cloud-Studie dargestellt.

Generell lässt sich jedoch festhalten: Wenn Daten auf dem eigenen Rechner verschlüsselt und erst dann ins Internet oder einen Cloud-Speicher gestellt werden, sind die Daten nicht auslesbar. Außerdem können Sicherheitsdienste aus der Cloud kleine und mittlere Unternehmen besonders gut schützen.

Fraunhofer SIT

Fraunhofer-Institut für Sichere Informationstechnologie
Rheinstraße 75 · 64295 Darmstadt
www.sit.fraunhofer.de



## » Sehe ich das Schloss im Browser, ist alles okay. «

Das Schloss in der Browserzeile sagt lediglich aus, dass eine verschlüsselte Verbindung (HTTPS) besteht. Über die Absichten der Gegenstelle oder über die Abwesenheit von Schadcode sagt es nichts aus. Denn viele Angriffe können auch über verschlüsselte Verbindungen erfolgen.

Beispielsweise kann eine sogenannte Man-in-the-Middle-Attacke erfolgen. Hierbei kann der Angreifer einen SSL-Proxy aufbauen und unbemerkt mithören oder Inhalte austauschen.

Für einen guten Schutz sollten daher das Betriebssystem und der Browser immer aktuell gehalten werden, damit auch die entsprechenden Zertifikate auf dem neuesten Stand sind.

Fraunhofer SIT

Fraunhofer-Institut für Sichere Informationstechnologie
Rheinstraße 75 · 64295 Darmstadt
www.sit.fraunhofer.de

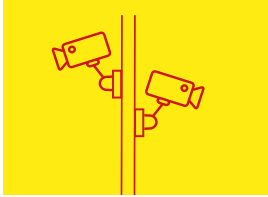
## » Gut ausgerüstete Hacker haben immer einen Eisschrank in ihrer Werkstatt. «

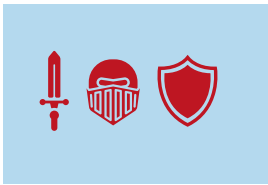
Es klingt ungewöhnlich, aber es stimmt, dass tiefgekühlte Speicherchips nützlich für Hacker sind. Die Daten im Speichermedium sind bei der Eiseskälte im Gefrierschrank nämlich weniger flüchtig.

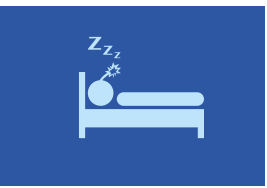
Versierte Hacker können so – mit der richtigen Vorgehensweise – verschlüsselte Partitionen von Smartphones und Laptops ohne Eingabe des passenden Schlüssels auslesen.

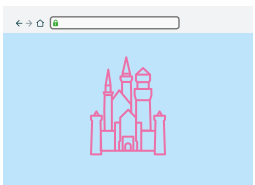
Fraunhofer SIT

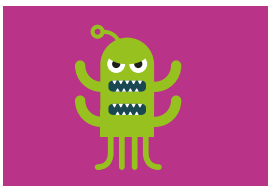
Fraunhofer-Institut für Sichere Informationstechnologie
Rheinstraße 75 · 64295 Darmstadt
www.sit.fraunhofer.de













Fraunhofer
SIT

Fraunhofer-Institut für Sichere Informationstechnologie
Rheinstraße 75 · 64295 Darmstadt
www.sit.fraunhofer.de