

BestBusiness-Mobility

INNOVATION UND MOBILITÄT FÜR LEISTUNGSFÄHIGE UNTERNEHMEN

powered by

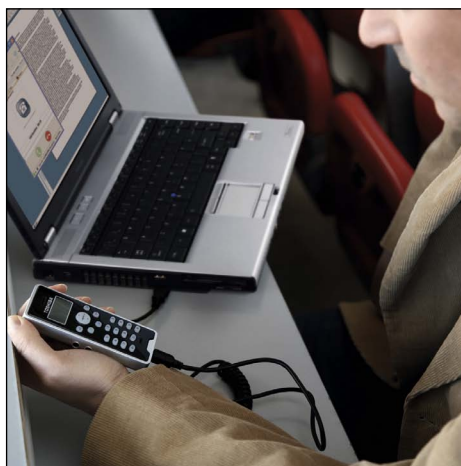
TOSHIBA
Leading Innovation >>>



SICHERHEIT



SICHERHEIT MIT KONZEPT – MOBILE INFRASTRUKTUREN SCHÜTZEN



Aus dem Inhalt

Vorwort/Geleitwort	3
Mobil – aber mit Sicherheit	4
Mobilität und Sicherheit im ganzen Unternehmen	5
Sichern Sie Ihr Unternehmen	8
Fünf entscheidende Pluspunkte für Toshiba-Business-Notebooks.	10
Zehn Tipps für eine sichere Mobilität	11

„Die Vorteile von Mobilität lassen sich nur dann wirklich ausschöpfen, wenn die Daten und die Geräte unterwegs auch entsprechend gesichert sind. Ohne ein Sicherheitskonzept ist Mobilität mehr Risiko als Chance.“

Impressum



Herausgeber:

pfg – performance for growth GmbH, Hofweg 6, D-22085 Hamburg, Telefon: (0 40) 41 92 91-83, Telefax: (0 40) 41 92 91-89, Lichtentaler Straße 25, D-76530 Baden-Baden, Telefon: (0 72 21) 9 96 44-0, Telefax: (0 72 21) 9 96 44-99, E-Mail: info@pfg-net.de; V. i. S. d. P. Martin Puscher; Bildhinweis: Toshiba Europe GmbH; © by pfg GmbH

Diese Broschüre einschließlich aller ihrer Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Herausgebers unzulässig und strafbar. Dies gilt insbesondere für die ganze oder teilweise Vervielfältigung, Bearbeitung, Übersetzung, Mikroverfilmung sowie die Einspeicherung oder Verarbeitung in elektronische Medien, elektronische Systeme oder elektronische Netzwerke. Alle Angaben, trotz sorgfältiger redaktioneller Bearbeitung, ohne Gewähr. Wir weisen darauf hin, dass hier verwendete Soft- und Hardwarebezeichnungen und Markennamen der jeweiligen Firmen im Allgemeinen warenzeichen-, marken- oder patentrechtlichem Schutz unterliegen.

In Zusammenarbeit mit:

BestPractice-IT
IMPULSGEBER FÜR DEN MITTELSTAND
www.bestpractice-it.de

Vorwort



„Auf Nummer sicher gehen,
um Chancen der Mobilität zu nutzen!“

Liebe Leserinnen
und Leser,

produktiv, flexibel und individuell – das ist Mobilität in ihrer idealen Form. Je mobiler Sie Ihre Geschäftsprozesse gestalten, desto größer sind die Potenziale, die Sie durch die Nähe zu Märkten, zu Kunden und Partnern oder durch kurze Entscheidungswege ausschöpfen können. Mobilität wird dabei immer mehr zu einer zentra-

len Anforderung, um zukunfts- und wettbewerbsfähig zu bleiben. Mit dieser Anforderung geht eine ganz entscheidende Notwendigkeit einher. Mit Ihren mobilen Mitarbeitern sind Daten unterwegs. Das können sowohl kundenbezogene als auch unternehmensspezifische Daten sein. Beide sind wertvoll, und Wertvolles gilt es zu schützen. Dies gilt für den Datenträger, also das mobile Endgerät. Gleichzeitig bedeutet Mobilität auch, die Funktionsfähigkeit der mobilen Infrastruktur SICHERzustellen.

Wir wollen daher mit diesem vorliegenden Guide gemeinsam mit Ihnen das Thema „Sicherheit“ zur Chefsache erklären. Nehmen Sie dieses Thema ernst. Nur dann können Ihre Kollegen und Mitarbeiter produktiv, flexibel und individuell arbeiten – sichern Sie Ihren Unternehmenserfolg.

Herzlichst, Ihr
Michael Sauer,
Vertriebsdirektor B2B,
Toshiba Europe GmbH
Computersysteme DACH

Geleitwort



Der überwiegende Teil unserer Geschäftsprozesse wird heute elektronisch gesteuert, Kundeninformationen und Unternehmens-

daten werden digital gespeichert. Mit der steigenden Erleichterung durch diese digitale Welt steigt aber auch das Gefährdungspotenzial, da immer mehr sensible Daten der Informationstechnik anvertraut werden. Mit zunehmender Mobilität der Mitarbeiter kommt eine weitere Dimension hinzu. Daten werden nicht nur digital versendet, sondern sind auch physisch unterwegs.

Das Thema IT-Sicherheit ist für Unternehmen aller Größenordnungen lebensnotwendig. Studien zeigen, dass vor allem der Mittelstand Ziel von

Sicherheitsangriffen ist. Dafür gibt es besonders zwei Gründe. Der Mittelstand in Deutschland ist ein zentraler Innovator und Hort für Geschäftsideen und -potenziale. Gleichzeitig ist der Mittelstand häufig auch ein leichtes Ziel, weil der Bereich Sicherheit nicht konsequent angegangen wird.

Mit dem IT-Grundschatz des BSI geben wir seit über 15 Jahren erfolgreich Hilfestellung beim Thema der IT-Sicherheit. Mit Maßnahmen-Katalogen, Checklisten und Schulungen geben wir konkrete Tipps und Hinweise, um Sicherheit zu gewährleisten. Über die Definition von Standards, Akkreditierungen und Zertifizierungen geben wir Unternehmerinnen und Unternehmen Instrumente an die Hand, mit denen sie sich als vertrauensvolle Geschäftspartner mit einem umfassenden Sicherheitskonzept positionieren können.

Sicherheit schafft Vertrauen – für eine sichere Informationstechnik in unserer Gesellschaft.

Ihr
Matthias Gärtner
Pressesprecher
Bundesamt für Sicherheit in der
Informationstechnik (BSI)



Mobil – aber mit Sicherheit

Nicht einmal jeder zwölfte Deutsche glaubt, dass seine Daten bei Unternehmen ausreichend geschützt sind. Dies ergab eine aktuelle Umfrage des Instituts für Demoskopie Allensbach. Die Datenschutzaffären der Vergangenheit haben offenbar Spuren hinterlassen. Kunden überlegen daher ganz genau, welche Daten sie beim Kauf von Produkten und bei der Bestellung von Informationsmaterial angeben.

Ein Blick hinter die Unternehmensmauern scheint die Kunden in Ihrer Skepsis zu bestätigen. Nach einer Umfrage des Sicherheitsunternehmens McAfee sieht die Mehrheit des deutschen Mittelstandes keine Gefahr durch Hackerangriffe und Internetkriminalität. Diese Gelassenheit ist aber ein Trugschluss, wie andere Studien belegen. Danach sind gerade kleinere Unternehmen besonders häufig im Visier von Hackern und somit Ziel der Angriffe. Doch nicht nur Kundendaten gilt es zu schützen. Kleine und mittlere Unternehmen sind häufig Triebfedern für innovative Entwicklungen und damit interessant für Industriespione. Der Schutz

des betrieblichen Wissens muss daher ein bedeutender Bestandteil in Ihrem Sicherheitskonzept sein. Stellen Sie sich nur vor, wenn Ihre neue Produktentwicklung, für die sie viel Zeit und Geld investiert haben, unerwartet – fast baugleich – bei Ihrem Wettbewerber auftaucht.

Zwar sind sich fast alle Unternehmer der Bedeutung von Sicherheit bewusst. Dennoch zeigen die bisherigen Investitionen in IT-Sicherheit, dass ein erheblicher Nachholbedarf besteht. Wunsch und Wirklichkeit passen hier nicht zueinander. Die Prognosen für die zukünftigen Entwicklungen zeigen aber, dass über Sicherheitskonzepte zumindest verstärkt nachgedacht wird. Es sind nicht alleine finanzielle Ressourcen, die bei einem geeigneten Sicherheitskonzept entscheidend sind. Das umfassende Sicherheitskonzept greift nur dann, wenn es auf Arbeits- und Geschäftsprozesse abgestimmt und ausgerichtet ist. Hinzu kommen auch die erweiterten Kommunikationsprozesse, die mit dem zunehmenden Einsatz mobiler Mitarbeiter und Endgeräte komplexer und damit angreifbarer werden. Mobile Endgeräte bedeuten:

- **mobile Daten und Information**
- **mobile Hardware**
- **mobile Kommunikation**

So ist es nicht verwunderlich, dass IT-Verantwortliche in mobilen Mitarbeitern das Sicherheitsrisiko Nummer 1 sehen, etwa durch den Remote-Zugriff auf das Firmennetzwerk oder die Kommunikation über WLAN und UMTS. Auch Wechseldatenträger und zusätzlich verwendete mobile Kommunikationsgeräte wie Smartphones tragen zu einem erhöhten Sicherheitsrisiko bei.

Aus betriebswirtschaftlicher Sicht führt jedoch kein Weg an mehr Mobilität vorbei, selbst wenn mobile Mitarbeiter den IT-Verantwortlichen häufig Kopfzerbrechen bereiten.

Ihre Daten auf Wanderschaft

Nähe zu den Märkten, Nähe zu Kunden – der mobile Arbeitsplatz ist Chance und Risiko zugleich. Ihre mobilen Mitarbeiter verlassen Ihren Firmensitz nämlich nicht alleine. Sie nehmen auf ihren mobilen Endgeräten Daten und Informationen mit. Ihre Daten sind also auf Wanderschaft.

Daten und Informationen sind zudem auch Teil der Kommunikation, sie werden versendet, von Mitarbeiter abgerufen, auf weiteren Geräten zwischengespeichert. Die Mikroelektronik macht es möglich, dass Ihre Mitarbeiter immer mehr Daten mit auf Reisen nehmen können, Breitband und UMTS ermöglichen den Abruf und das Versenden großer Datenmengen. Die heutigen technischen Voraussetzungen machen das mobile Büro zur Realität. Doch Ihr Büro wird damit zugänglich. Damit sind nicht nur andere Menschen gemeint, sondern auch Umwelteinflüsse. Ein mobiles Büro ist anfälliger als ein physisches. Um den größtmöglichen Schutz gewährleisten zu können, müssen wir die Risiken kennen, um mögliche Gefahren abzuwehren.

Analysen zeigen, dass gerade der Kommunikation zwischen Unternehmen und den mobilen Mitarbeitern nicht ausreichend Aufmerksamkeit geschenkt wird.

Aufgrund der Vielzahl von Risiken und Bedrohungen verlangt Sicherheit nach der Entwicklung, Etablierung und Aktualisierung eines Gesamtkonzeptes. Sicherheit bedeutet nicht nur, ein Antivirenprogramm auf Notebooks zu installieren oder das Unternehmensnetzwerk durch eine Firewall zu schützen. Sicherheit ist vor allem eines: **Sicherheit ist Chefsache!**

Mobilität und Sicherheit im ganzen Unternehmen

Sicherheit bedeutet auch Vorsicht. Vorausschauendes Handeln ist notwendig, um für die Risiken des mobilen Arbeitens gewappnet zu sein. Die Herausforderungen für die richtige Sicherheitsstrategie sind für die unterschiedlichen Zielgruppen im Unternehmen verschieden.

Kaufmännischer Entscheider

Sicherheit ist Vertrauen – Nutzung der richtigen Partner

Mittelständische Unternehmen verlassen sich häufig auf leistungsstarke Partner, wenn es um ihre IT geht. In Sicherheitsfragen muss dies im wahrsten Sinne des Wortes der Partner „Ihres Vertrauens“ sein. Es ist also ratsam, das Gespräch mit potenziellen Systemhäusern und Resellern zu suchen, um daraus den für Sie geeig-

netsten Anbieter zu wählen. Haben Sie schon einen langjährigen Partner, dann sind Sie bereits gut bedient, wenn es in der Vergangenheit keine kritischen Sicherheitsvorfälle gab. Arbeiten Sie gemeinsam ein Sicherheitskonzept aus, das neben den Endgeräten auch die notwendige Softwareunterstützung sowie Sicherungs- und Updatefunktionen beinhaltet.

Vertrauen auf eigene Ressourcen vs. Vertrauen in fremde Ressourcen

Durch die Auslagerung und damit die Nutzung der Managed Security Services lässt sich der Aufwand im Unternehmen reduzieren, gleichzeitig aber der Sicherheitsstandard durch die Professionalisierung erhöht. Die Sicherung Ihrer Infrastruktur wird von einem Partner übernommen. Natürlich ist dabei Vertrau-



en ein wesentlicher Gesichtspunkt, doch vertrauensbildend ist alleine schon der Aspekt, dass ein Lösungsanbieter an einer langfristigen Beziehung zu Ihnen interessiert ist und daher kaum geneigt sein wird, Ihr Vertrauen zu missbrauchen. Ein weiterer Vorteil an diesem Modell ist

Gefahr für Ihre Daten und Geräte

virtuell	physisch
<p>Datendiebstahl Wirtschaftskriminalität über Hackerangriffe, Ausspionierung von Daten über Spyware oder Trojaner: Studien belegen, dass die Computerkriminalität ein blühendes Wachstumsgeschäft ist. Untersuchungen gehen dabei von einem gesamtwirtschaftlichen Schaden von nicht weniger als 100 Milliarden Euro in Deutschland aus.</p>	<p>Unfälle Fast die Hälfte aller Defekte bei Notebooks sind auf einen Sturz des Gerätes zurückzuführen. Doch auch ein verschüttetes Getränk kann einen ähnlichen Effekt haben. Zwar landen die Daten dabei nicht in fremden Händen, doch kosten sowohl das Notebook als auch die Datenwiederherstellung viel Geld.</p>
<p>Datenschädigung Die Gefahr durch Viren variiert von einfachen Schädigungen, wie etwa die Störung der Druckfunktion oder PDF-Erstellung, bis hin zur Lösung von Kundendatenbeständen. Die Wirkungen reichen dabei dann von Ärger und Zeitaufwand bis zu massiven Kosten aufgrund verlorener Datenbestände.</p>	<p>Diebstahl/Verlust Einmal unachtsam und schon ist das Notebook weg. Über 40 % der Datenverluste lassen sich auf den Diebstahl oder das Liegenlassen eines Notebooks zurückführen. Bedenkt man dabei, dass ein verlorenes mobiles Endgerät aufgrund des Eigenwertes und der gespeicherten Daten Unternehmen im Schnitt 50.000 Euro kostet, erhält diese Gefahr eine erhebliche Bedeutung.</p>

Der größte Risikofaktor für Ihre mobilen Daten und Geräte ist zusammengefasst Ihr Mitarbeiter selbst. 70 bis 80 % der Schäden entstehen durch die eigenen Mitarbeiter. Dies ist zum Teil der Notwendigkeit von Mobilität geschuldet. Nach einer Studie von TrendMicro neigen mobile Anwender eher zu einem riskanteren Online-Verhalten als Desktop-Nutzer. So gaben 54 % der deutschen Laptop-Nutzer an, schon einmal ausführbare Dateien über das Unternehmensnetzwerk heruntergeladen zu haben. Bei Desktop-Nutzern waren es lediglich 41 %.

Verschlüsselung macht Daten sicherer

FOKUS

Einen wichtigen Brief, Rechnungen oder Verträge lassen Sie sicherlich nicht offen auf dem Schreibtisch liegen. Wichtige Dokumente verschließen Sie sogar in einem Safe. Ähnlich müssen Sie aber auch die wichtigen Dokumente und Daten schützen, die Sie digital abgelegt und gespeichert haben. Verschlüsselungsmethoden sind hierbei eine wirksame Methode, Ihre Daten vor unbefugten Zugriffen zu sichern, selbst wenn das Notebook doch einmal verloren geht oder gestohlen wird.

Bei der Verschlüsselung einer Datei wird diese mittels eines Algorithmus und einer oder mehrerer Zahlen- und Buchstabenkombinationen verfremdet. Die Dateientschlüsselung kehrt diesen Vorgang wieder um. In gleicher Weise lässt sich auch die gesamte Festplatte verschlüsseln. Die Codierung und Verschlüsselung gesamter Datenbestände hat den Vorteil, dass der Decodierungsvorgang und eine Passwortabfrage nur einmal getätigt werden müssen, um dann bis zum nächsten Neustart mit den gesamten Daten und Informationen arbeiten zu können.

Heutige Tools nutzen symmetrische Verschlüsselungen, bei denen derselbe Schlüssel zum De- und Encodieren dient. Als aktueller Stand der Technik

gilt der Algorithmus Advanced Encryption Standard (AES), der in den USA z. B. auch für die Sicherung von Dokumenten mit höchster Geheimhaltungsstufe eingesetzt wird.

Beim mobilen Arbeiten lohnt es sich auch, über eine Verschlüsselung von besonders wichtigen E-Mails nachzudenken, um unerwünschtes Mitlesen auszuschließen. Hier greift das sogenannte Public-Key-Verfahren. Benötigt werden zwei Schlüssel, ein sogenannter öffentlicher zum Verschlüsseln und ein geheimer zum Entschlüsseln empfangener Mails. Den öffentlichen Schlüssel können Sie an Ihre Geschäftspartner und Mitarbeiter weitergeben. Damit können diese dann die Mails verschlüsseln, danach aber nicht mehr entschlüsseln. Dies ist nur mit dem privaten, geheimen Schlüssel möglich.

Sichere Korrespondenz und Schutz der Daten sind aber nur dann wirksam, wenn die damit verbundenen Passwörter gut gewählt und gut gehütet werden. Klar ist, dass gute Passwörter nicht immer gut zu merken sind. Wenn Sie Passwörter speichern, dann ebenfalls nur an sicheren Orten! Sie lassen auch nicht Ihren Haustürschlüssel von außen stecken, wenn Sie aus dem Haus gehen.

die Möglichkeit der bedarfsgerechten Beschaffung. Da Sie die Sicherheitslösungen und Sicherheitskomponenten mieten, ist es einfacher, eine maßgeschneiderte Lösung für Sie zu entwickeln. Diese enthält dann im Gegensatz zu Softwarepaketen nur die Komponenten, die Sie tatsächlich benötigen. Machen Sie diese Entscheidung von Ihrem Know-how im eigenen Unternehmen und den Angeboten und Kompetenzen Ihrer Partner abhängig. Bereits auf dem Weg zur Beantwortung der Frage „Selbst machen oder auslagern?“ erfahren Sie viel über die Anforderungen und Notwendigkeiten im Bereich der IT-Sicherheit.

Sicherheitsstrukturen schaffen – Mitarbeiter mitnehmen

Der Unternehmer ist gefordert, wenn es um die Erstellung von Richtlinien für die IT-Sicherheit geht. In Absprache mit dem IT-Verantwortlichen müssen die Mitarbeiter für den sicheren Umgang mit Daten sensibilisiert werden. Der Verlust oder Diebstahl eines Gerätes ist umgehend zu melden.

Wie so oft ist auch beim Thema der Richtlinien die Balance zwischen hohen Sicherheitsstandards und flexiblen Arbeitsmethoden zu suchen. Zusätzlich muss Einigkeit über die doppelte Nutzung („Dual Use“) mobiler Endgeräte erzielt

werden. Einem Vertriebsmitarbeiter, der eine Woche unterwegs ist, muss auch die Möglichkeit der privaten Nutzung eingeräumt werden.

IT-Entscheider

Umfassender Schutz – nutzen was möglich ist

Häufig sind bereits werkseitig viele Sicherheitskomponenten in mobilen Endgeräten integriert. Es ist etwa ratsam, das BIOS-Bootpasswort zu aktivieren oder die Festplatte zu verschlüsseln. Gleichzeitig ist es natürlich wichtig, die Benutzerfreundlichkeit nicht gänzlich zu strapazieren. Aber im Zweifelsfall gilt: Ein Passwort zu viel hat noch niemandem geschadet – eines zu wenig dagegen schon.

Die auf allen Toshiba Notebooks vorinstallierte Lösung Computrace-One von Absolute Software bietet im Falle eines Diebstahls oder Verlustes über den BIOS-Agent größte Chancen, das Gerät aufzuspüren und somit zurückzuholen. Aktivieren Sie diese selbstreparierende, persistente Lösung auf Ihren mobilen Endgeräten, tragen Sie zum Diebstahlschutz bei und minimieren zugleich über die Möglichkeiten der Datenfernlöschung die unbefugte Verwendung Ihrer Daten.

Um die sichere Kommunikation zwischen mobilen Mitarbeitern und dem Firmennetzwerk zu gewährleisten, muss der IT-Verantwortliche besonders auf die sich bietenden Möglichkeiten der Datenverschlüsselung (die Anbindung an das Firmennetzwerk sollte idealerweise nur per SSL-VPN oder IPSec erfolgen) zurückgreifen. Zudem muss überprüft werden, welche Dienste, Applikationen und Schnittstellen wirklich benötigt werden. Nicht benötigte Dienste, wie etwa der Ad-hoc-Modus beim WLAN, sind zu deaktivieren. Die verwendeten WLAN-Geräte müssen den Standard 802.11i unterstützen, damit eine Verschlüsselung per WAP2 erfolgen kann.

Mit Aktualität gegen Schädlinge und Schäden

Die Dynamik der Computerkriminalität bedeutet, dass täglich neue Bedrohungen zu den aktuellen hinzukommen. Trojaner, Viren, Spyware, die Bedrohungen kommen

aus ganz unterschiedlichen Richtungen mit ganz unterschiedlichen Zielsetzungen. Notwendig ist dabei eine leistungsstarke, aktuelle und umfassende Sicherheitssoftware, die immer auf dem neuesten Stand gehalten werden muss. Bei mobilen Endgeräten kann dies entweder über die Fernwartung (diese bieten leistungsstarke Partner an) oder über ein Update des Gerätes bei Rückkehr ins Unternehmen erfolgen. Hier gilt es auch, den mobilen Mitarbeiter zu schulen, welche Updates er selbst machen sollte, und ihn mit den entsprechenden Rechten auszustatten.

Rechte einräumen und Rechte zuweisen – den richtigen Umgang definieren

Allerdings ist der Umgang mit Rechten immer ein Balanceakt. Zu viele Rechte steigern das Sicherheitsrisiko, zu wenige Rechte hemmen den Arbeitsfluss und erhöhen den administrativen Aufwand. Ausführliche Planung und ausreichende Testphasen erhöhen zwar zu Beginn des neuen Rechtemanagements den Aufwand, erleichtern aber zukünftig die Bedienung und Administration und senken damit wirkungsvoll den Folgeaufwand. Die Definition des richtigen Umgangs bedeutet aber auch eine regelmäßige Prüfung der Softwarebedürfnisse und Programmstrukturen eines mobilen Endgerätes. Programmupdates oder neu benötigte Software müssen daher immer aktuell und zeitnah installiert werden, um zu verhindern, dass mobile Mitarbeiter selbstständig Programme, Add-ons etc. aus möglicherweise nicht vertrauenswürdigen Quellen herunterladen müssen.

Zu einem sinnvollen Rechte-Management gehört auch eine Authentifizierung des Nutzers gegenüber seinem mobilen Gerät, etwa über biometrische Verfahren oder Smartcards zu realisieren. Bei der Authentifizierung sollte mindestens eine 64-bit-Verschlüsselung verwendet werden.

IT-Anwender

Das Notebook als Wertgegenstand – Wertvolles schützen

Dem Anwender kommt bei der IT-Sicherheit die wichtigste Rolle zu, denn er ist der Träger und Verwahrer der Daten. Wer diese Verantwortung trägt, muss sein Ver-

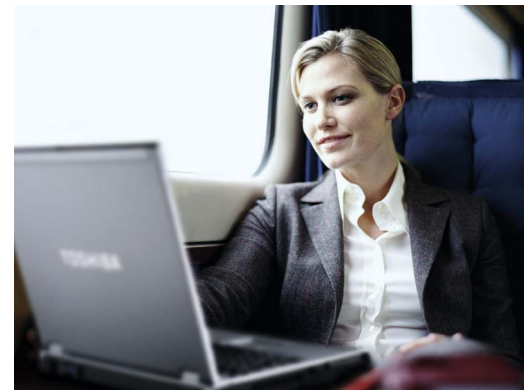
halten entsprechend darauf abstimmen. Das Online-Verhalten und der Umgang mit Daten müssen dem Rechnung tragen. Das gilt auch für die Beaufsichtigung des Notebooks. Es sollte niemals ungesichert liegen gelassen werden. Solche Momente müssen nicht zwangsläufig zum Diebstahl führen. Es besteht auch die Gefahr, dass jemand Einsicht in Daten nimmt oder entsprechende Spyware installiert. Gibt man das Notebook aus der Hand, muss es besonders gesichert sein. Idealerweise sollten die zentralen Daten auf dem Unternehmensserver oder einem Wechsel Datenträger gespeichert werden, den der Mitarbeiter dann bei sich trägt.

Das Notebook als Gebrauchsinstrument und nicht als Verbrauchsgegenstand

Der richtige Umgang mit Betriebskapital ist sehr wichtig. Natürlich muss der Mitarbeiter mit entsprechenden Transportmöglichkeiten (Tasche, Schutzhüllen etc.) ausgestattet sein. Doch liegt es in seiner Verantwortung, das Notebook pfleglich zu behandeln. Toshiba Notebooks können schon mal einen Stoß vertragen. Dafür sorgen in den Business-Notebooks extrastarke Scharniere, robuste Gehäuse und innovative Sicherheitsmechanismen, wie z. B. Bewegungssensoren, die einen Festplatten-Crash verhindern. Toshiba ist als Begründer der EasyGuard-Technologie seit jeher ein Trendsetter und Innovator für mobile Sicherheit. Darauf können Sie sich auch in Zukunft verlassen.

So bleiben Ihre Mitarbeiter sicher und mobil – mit perfekt verwalteten Notebooks.

Da bei der Intel® Centrino® 2 und vPro™ Technologie Sicherheits- und Systemverwaltungsfunktionen direkt im Chip integriert sind, können Sie mittels hardwaregestützter Funktionen die Notebooks Ihrer Mitarbeiter per Fernzugriff isolieren und überprüfen, sowie Fehler beheben, selbst wenn das Betriebssystem nicht reagiert. Und die herausragende Dualcore-Leistung ermöglicht mehr Geschwindigkeit in drahtlosen Netzen und Verbesserungen bei der Akkulaufzeit. ■



Die Versicherung Ihrer Mobilität: Toshiba EasyGuard

Toshiba EasyGuard fokussiert auf drei Notebook-Sicherheitsthemen:

- Secure

„Secure“ als Bestandteil ist komplett auf die erweiterte System- und Datensicherheit fokussiert. Die Password-Utilities bieten die Möglichkeit der Einrichtung zusätzlicher Passwörter für die Festplatte oder für den Bootvorgang. Device Access Control schützt vor unbefugtem Zugriff auf den Computer oder vor dem unbefugten Kopieren vertraulicher Daten.

- Protect and Fix

Die integrierten Schutzvorrichtungen und Diagnose-Utilities von Protect and Fix gewährleisten erweiterten Systemschutz und maximale Online-Zeiten: z. B. durch eine spritzwassergeschützte Tastatur oder das Shock Protection Design, mit dem Ihr Notebook gegen die Folgen von Stößen geschützt ist.

- Connect

Durch den leichten und komfortablen Zugang über das Tool Config-Free bleiben „waghalsige“ Einwahlvorgänge in unsichere Netze aus, da auch technisch nicht versierte Mitarbeiter problemlos Verbindungen herstellen können.

Sichern Sie Ihr Unternehmen

Feature	Nutzenbeschreibung
3-D-Festplattenschutz	Schützt vor Datenverlust bei Erschütterungen und Sturz
Robustes Design	Verbesserte Produktqualität, Zuverlässigkeit und Haltbarkeit
Spritzwassergeschützte Tastatur	Ermöglicht mehrere Minuten lang das sichere Herunterfahren nach Wasserkontakt und schützt dadurch vor Daten - und/oder Geräteverlust
Stoßfestes Design	Polsterung schützt Gerätekomponenten bei Erschütterungen
eSATA	Ermöglicht den Anschluss sehr schneller externer Festplatten
WLAN-Schalter	Schalter für einfaches Bedienen der Konnektivitätsmodule
Intel® Centrino® 2 mit vPro™ Technologie	Größere Rechenleistung, Rechnerbeschleunigung
Ausfallraten	Durch spezielle Qualitätssicherungsverfahren werden die Ausfallraten der Geräte reduziert; dies führt zu Kostenersparnis und sorgenfreies Computing beim Anwender
HALT-Test	Verbessert die Serienproduktionsqualität und führt zu zuverlässigeren Geräten
BIOS mit Computrace®-Unterstützung	Optional erhältlich, ermöglicht dieses Feature das Suchen, Finden und Wiedererlangen gestohlener Notebooks.
Diebstahlschutz durch Toshiba BIOS-Timer	BIOS-Passwort schützt vor Systemzugriffen nach Diebstahl; ein Aufkleber auf dem Display-Deckel soll potenzielle Diebe vorab darauf hinweisen
Intel® Active Management Technologie 4.0 (iAMT 4.0)	Erhöht die Sicherheit außerhalb des Firmennetzwerks und gegen Angriffe
Password Utilities	Leichtes Einrichten der Passwörter für Bootvorgang und Festplattenzugriff
Toshiba Device Access Control (auf Anfrage)	Ermöglicht das flexible Sperren spezifischer Geräte und Ports gegen Computerzugriff oder Kopieren von Daten
Intel® Active Management Technologie 4.0 (iAMT 4.0)	Diese hardwarebasierte Technologie hilft, Wartungskosten und Ausfallzeiten stark zu senken und Richtlinien zu halten; sie kann Vor-Ort-Wartungszeiten um mehr als 50 % reduzieren.
Intel® Virtualization Technology	Ermöglicht das Erstellen unterschiedlicher virtueller Notebooks, um zum Beispiel berufliche und private Bereiche klarer voneinander zu trennen
PC Diagnostic Tool	Speziell entwickelte Toshiba Software für den Zugriff auf den Systemsupport und die Systemdienste per Tastendruck, um die Wartungskosten zu senken und die Ausfallzeiten des Systems zu minimieren
Toshiba Management Console	Notebooks können aus der Ferne aktualisiert und verwaltet werden, sodass Ausfallzeiten reduziert und die Produktivität gesteigert wird
Toshiba Power Saver Utility	Ermöglicht dem Benutzer, Leistung und die Akkubetriebszeit an den aktuellen Bedarf anzupassen
EasyClean	Optimale Kühlung der Systeme durch einfache Reinigung des Lüfters

Erläuterung der Legende:

★★ – hoher Beitrag zum Nutzen, ★ – wichtiger Beitrag zum Nutzen

Technikbeschreibung	Fördert die Betriebssicherheit	Erhöht die Datensicherheit
Der 3-D-Beschleunigungssensors erkennt einen freien Fall, Stoßeinwirkungen oder Erschütterungen des Geräts in jeglicher Richtung: tritt der Fall ein, wird der Festplattenkopf blitzschnell von den Platten entfernt und der Aufprall vorbereitet, um den Verlust wertvoller Daten zu vermeiden	★★	★★
Das robuste Systemdesign garantiert verbesserte Produktqualität, Zuverlässigkeit und Haltbarkeit	★	
Die spritzwassergeschützte Tastatur schützt das System vor verschütteten Flüssigkeiten und gibt dem Benutzer mehrere Minuten Zeit, um alle offenen Dateien zu schließen und den Rechner auszuschalten	★★	★★
Kernkomponenten wie Festplatte, Display und Inverter werden durch Luftpolsterung und eine spezielle Ummantelung geschützt – das Gehäuse schützt das Notebook und die Daten vor kleineren Stößen und Schlägen im täglichen Betrieb	★★	★★
Dieser Anschluss ermöglicht es, sehr schnelle externe Festplatten an das Notebook anzuschließen, um z. B. Back-ups in sehr kurzer Zeit zu fahren	★	
Schalter für die einfache und sichere Aktivierung/Deaktivierung der integrierten WLAN-, 3G oder Bluetooth®-Module		★★
Im Vergleich zu Generation Intel® Centrino® mehr als doppelte CPU-Performance bei CPU-intensiven Aufgaben (durch fünf Intel Core 2 Duo Prozessoren mit einem L2-Cache von bis zu 6 MB und einem 1.066 MHz schnellen Front Side Bus)	★	
Durch spezielle Qualitätssicherungsverfahren werden die Ausfallraten der Geräte reduziert. Dies führt zu Kostenersparnis und sorgenfreies Computing beim Anwender	★★	
Durch spezielle Testverfahren vor Beginn der Serienproduktion wird die Alterung der Geräte simuliert; dadurch können eventuelle Schwachstellen vor Beginn der Serienproduktion identifiziert und die Zuverlässigkeit und Langlebigkeit der Geräte erhöht werden	★★	
Diese unauffällige, mehrschichtige Sicherheitslösung ist optional erhältlich und ermöglicht das Suchen, Finden und Wiedererlangen gestohlener Notebooks	★	★★
Der BIOS-Timer macht das Gerät nach einem vorher einzustellenden Countdown unbrauchbar und erfordert dann die Eingabe des BIOS-Passworts; ein Aufkleber auf dem Display-Deckel soll potenzielle Diebe vorab darauf hinweisen	★	★★
IT-Abteilung kann auch außerhalb der unternehmenseigenen Firewall sicher kontaktiert werden; durch programmierbare Hardware-Datenfilter mehr Schutz vor Viren und Attacken	★	★★
Toshiba Software-Utilities, mit denen Systemadministratoren und Benutzer Passwörter für Bootvorgang und Festplattenzugriff einrichten können	★★	★★
Softwareprogramm für das flexible Sperren spezifischer Geräte und Ports, um den unberechtigten Computerzugriff oder das Kopieren vertraulicher Dateien zu verhindern.	★	★★
Notebooks können im Schlafmodus aus der Ferne und außerhalb regulärer Betriebszeiten aufgeweckt, verwaltet und konfiguriert werden; auch infizierte PCs; auch nicht reagierende Betriebssysteme; Notebooks mit der Technik lassen sich mit allen bedeutenden System-Managementprogrammen integrieren und unterstützen die Standards der nächsten Generation Distributed Management Task Force DASH 1.0 für verbesserte Interoperabilität und Web Services Management (WS-MAN)	★	★
Alle virtuellen Systeme können mit diesem System bequem verwaltet werden - berufliche und private Bereiche können eingerichtet und unabhängig voneinander ausgeführt werden.	★	★★
Speziell entwickelte Toshiba Software für den Zugriff auf den Systemsupport und die Systemdienste per Tastendruck, um die Wartungskosten zu senken und die Ausfallzeiten des Systems zu minimieren	★★	
System- und Softwareinformationen werden vom Client erfasst, um die zentrale Aktualisierung des BIOS über ein Servermodul zu ermöglichen – Notebooks können aus der Ferne aktualisiert und verwaltet werden, sodass Ausfallzeiten reduziert und die Produktivität gesteigert wird	★★	
Das exklusive Toshiba Power Management ermöglicht dem Benutzer, verschiedene Einstellungen vorzunehmen, um die Leistung und die Akkubetriebszeit bedarfsgerecht einzustellen	★	
Optimale Kühlung der Systeme durch einfache Reinigung des Lüfters	★★	

Fünf entscheidende Pluspunkte für Toshiba Business-Notebooks

Auf den ersten Blick scheint die technische Ausstattung von Notebooks für Geschäftskunden identisch, z. B. bei Prozessor, Festplattenkapazität oder Arbeitsspeicher. Aber ein Toshiba Business-Notebook hat über die reinen technischen Daten hinaus viel mehr zu bieten.

Qualität

Business-Notebooks werden im mobilen Arbeitsalltag hohen Belastungen ausgesetzt. Deshalb werden Toshiba Business-Notebooks mit dem HALT-Test (Highly Accelerated Life Test) auf lange Lebensdauer getestet. Mit diesen Tests wird die Widerstandsfähigkeit gegen extreme Temperaturen, Vibrationen, Stöße oder Herunterfallen optimiert.

Sicherheit

Toshiba Notebooks bieten anspruchsvollen Geschäftskunden zahlreiche Sicherheitsfunktionen (z. B. Toshiba EasyGuard), die den tagtäglichen Einsatz der Notebooks entscheidend sicherer machen. Sie schützen z. B. wertvolle Daten vor Diebstahl, fremdem Zugriff oder auch Datenverlust.

Funktionalität

Im Businessseinsatz ist es besonders wichtig, die Bedienung der Notebooks so einfach und unkompliziert wie möglich zu machen. Zahlreiche benutzerfreundliche Features lassen Toshiba Kunden auf das Wesentliche konzentrieren – ihre Arbeit.

Konnektivität

Mit Toshiba Business-Notebooks können Ihre Kunden immer in Verbindung bleiben. Je nach Modell versenden und empfangen sie Daten über HighSpeed UMTS, Bluetooth®, WLAN und LAN. Besonders hilfreich ist dabei Toshiba ConfigFree™, eine Sammlung praktischer Technologien, die es dem User leicht machen, immer die optimale Verbindung zu finden und eventuelle Probleme zu lösen.

Daten- und Systemschutz

Der Schutz der wertvollen Daten hat bei professionell genutzten Notebooks oberste Priorität. Je nach Modell kommen besondere Schutzmerkmale zum Einsatz, z. B. Magnesiumgehäuse, spritzwassergeschützte Tastaturen, 3-D-Festplattenschutz und vieles mehr. ■



Die vier Business-Produktkategorien im Überblick

BUSINESS ALLROUNDER	BUSINESS PROFESSIONALS
Satellite-Pro-Serie	Tecra-Serie
<ul style="list-style-type: none"> • 13,3"-, 15,4"- und 17"-Displays • Docking über USB Docking „DynaDock“ • TruBrite® oder entspiegelte Displays • TouchPad 	<ul style="list-style-type: none"> • 14,1"- und 15,4"-Displays • Komfortable Dockinglösung über Express Port Replicator • Entspiegelte Displays • Dual Pointing (nicht bei Tecra R10) • Extrem robust und zuverlässig • Garantierte Plattform- und Imagestabilität von 12 Monaten • Erweiterte Toshiba EasyGuard Funktionen, z. B. spritzwassergeschützte Tastatur und Stoßabsorption bei Stürzen
DÜNN & LEICHT	TABLET PC
Portégé-Serie	Portégé-Serie
<ul style="list-style-type: none"> • 12,1" und 13,3" Displays • Ultraportabel und leicht • Ab 1,1 kg Gewicht! • Voll ausgestattet, inkl. DVD-Supermultilaufwerk • Innovative Technologien 	<ul style="list-style-type: none"> • 12,1" drehbares Display • Eingabe per Stift oder Tastatur • Docking über Express Port Replicator • Entspiegeltes Display

Für weitere Informationen besuchen Sie gerne unsere Mittelstandsseite im Internet: www.toshiba.de/mittelstand.

Haben Sie einen konkreten Beratungsbedarf, erreichen Sie uns unter:

Infoline Deutschland: 01805 96 90 10 (14 Cent/min aus dem deutschen Festnetz, ggf. abweichende Preise aus dem Mobilfunk)

Infoline Österreich: 0810 96 90 10 (10 Cent/min aus dem Festnetz der Telekom Austria)

Gerne können Sie uns auch eine E-Mail schreiben: info-computer@toshiba.de. Wir setzen uns dann schnell mit Ihnen in Verbindung.

Zehn Tipps für eine sichere Mobilität!

- **Wahl der Infrastruktur:** Vertrauen beginnt bereits bei der Wahl des mobilen Endgerätes. Verlassen Sie sich hier und bei der gesamten technischen Einführung auf einen Partner, mit dem Sie entweder bereits langfristig und erfolgreich zusammenarbeiten oder einen Partner mit einem guten Renommee.
- **Standards schaffen:** Häufig nutzen mobile Mitarbeiter ganz unterschiedliche Endgeräte, haben verschiedene Programme installiert und nutzen u. U. jeweils andere Sicherheitssoftware.
- **Mitarbeiter mitnehmen und sensibilisieren:** Schaffen Sie Richtlinien für den Internetgebrauch unterwegs und kommunizieren diese auch.
- **Geräteauthentifizierung:** Bei der Geräteauthentifizierung wird ein Gerät einem eindeutigen Nutzer zugewiesen. Damit erreichen Sie einen Schutz vor unbefugten Zugriffen.
- **Passwortüberprüfung:** Passwörter sollten regelmäßig auf ihre Sicherheit überprüft werden. So könnten Dritte aus dem Unternehmen befragt werden, welches Passwort sie bei einem Kollegen vermuten.
- **Funknetzübertragungen abschalten:** Wenn eine Verbindung nicht benötigt wird, sollte sie auf deaktiv eingestellt werden.
- **Ruhemodus absichern:** Nutzen Sie die Passwortfunktion von Bildschirmchonern oder die Passwortaufforderung beim Reaktivieren eines Gerätes aus dem Sleep-Modus.
- **Geschützte Wechselmedien nutzen:** Hier bietet es sich an, die Mitarbeiter mit unternehmenseigenen, verschlüsselten Wechselmedien auszustatten und nur diese zuzulassen.
- **Automatische Verschlüsselung:** Notwendig ist eine automatische und vollständige Verschlüsselung der Daten auf dem Notebook. Hierfür gibt es eine Reihe von leistungsstarken Lösungen.
- **Regelmäßige Sicherung:** Ein regelmäßiges Daten-Back-up sichert für den Ernstfall ein erleichtertes Recovery.

Ein Zusatztipp: Sicherheit darf nicht lähmen. Aufmerksamkeit, das richtige Konzept, die richtigen Partner und Vertrauen sind die Grundvoraussetzungen dafür, dass Sie und Ihre Mitarbeiter SICHER sein können, die Chancen von Mobilität komplett ausschöpfen zu können. ■



➤ **EIGENTLICH SCHADE,
DASS UNSERE NOTEBOOKS
NICHT KAPUTT GEHEN.**

**TOSHIBA DOPPELGARANTIE.
VOLLER KAUFPREIS ZURÜCK
& REPARATUR KOSTENLOS.**

Weil wir auf die Tecra A10 mit Intel® Centrino® 2 und vPro™ Technologie so sehr vertrauen, schenken wir unseren Geschäftskunden die Doppelgarantie.

Sollte Ihre Tecra A10 im ersten Jahr nach dem Kauf zu Garantiefall werden, dann bekommen Sie den vollen Kaufpreis und Ihr kostenlos repariertes Gerät zurück.

Die ganze Story unter:
www.toshiba.de/doppelgarantie



**Alles im
Griff**

**Toshiba empfiehlt
Windows Vista®
Business**



TOSHIBA
Leading Innovation >>>



**Ihre Vorstellung
von sauber**

ist
nicht
wie



**unsere Vorstellung
von sauber.**

Räume ordentlich und sauber zu halten ist schwer. Bei der Herstellung von Mikroprozessoren ist absolute Reinheit jedoch von größter Bedeutung. Für unsere mikroskopischen Transistoren ist das kleinste Staubkörnchen vergleichbar mit einem zwei Tonnen schweren Brocken. Deshalb sind unsere Reinräume 10.000 Mal reiner als ein OP. Und deshalb müssen unsere Arbeiter auch diese albernern Anzüge tragen. Erfahren Sie mehr auf www.intel.de/morgen.



Wir machen morgen möglich.™