dynabook

TOSHIBA

Sicheres Arbeiten für mobile Mitarbeiter

Sicherheit für mobile Mitarbeiter: **Einführung**

Unternehmen setzen vermehrt auf Edge-Computing-Modelle, bei denen immer leistungsfähigere Geräte die Daten lokal verarbeiten, anstatt sie an externe Server zu senden

Wir stehen am Beginn eines neuen Zeitalters hinsichtlich der mobilen Arbeit. Neueste technologische Entwicklungen in den verschiedensten Bereichen machen es immer einfacher, Dinge von zu Hause aus, unterwegs oder an anderen Orten außerhalb eines Büros zu erledigen. Mobile Geräte werden zunehmend leistungsfähiger – von Smartphones über Tablets bis hin zu Notebooks. Moderne Notebooks sind häufig unglaublich dünn und können fast so einfach wie ein Tablet in die Tasche gesteckt werden. Die Entwicklung stromsparender Technologien sorgt dafür, dass Akkus für die Anforderungen der meisten geschäftlichen Nutzer heutzutage lange genug fernab der Steckdose durchhalten.

Wir stehen am Beginn eines neuen Zeitalters hinsichtlich der mobilen Arbeit. Neueste technologische Entwicklungen in den verschiedensten Bereichen machen es immer einfacher, Dinge von zu Hause aus, unterwegs oder an anderen Orten außerhalb eines Büros zu erledigen. Mobile Geräte werden zunehmend leistungsfähiger – von Smartphones über Tablets bis hin zu Notebooks. Moderne Notebooks sind häufig unglaublich dünn und können fast so einfach wie ein Tablet in die Tasche gesteckt werden. Die Entwicklung stromsparender Technologien sorgt dafür, dass Akkus für die Anforderungen der meisten geschäftlichen Nutzer heutzutage lange genug fernab der Steckdose durchhalten.

Auch die Netzanbindung über WLAN-Hotspots oder Mobilfunkverbindungen wird immer schneller. Hotspots breiten sich vermehrt aus, und die meisten Smartphones integrieren den 4G-Standard. Mit 5G können Daten noch schneller ausgetauscht werden – mit bis zu 100 Megabit pro Sekunde, und diese Zahl wird wahrscheinlich in Zukunft noch steigen. Laut Ericsson wird es bis 2022 über 500 Millionen 5G-Teilnehmer geben.

Diese Netzanbindung eröffnet einem breiteren Personenkreis den einfacheren Zugriff auf immer größere Datenmengen. Die Kombination von schneller Netzanbindung und Cloud hat die Zusammenarbeit innerhalb von Unternehmen gefördert. Untersuchungen von Sky High haben gezeigt, dass mehr als 40 Prozent aller Dokumente in der Cloud nun von mehreren Mitarbeitern gemeinsam genutzt werden. Dies steigert die Produktivität und ermöglicht flexibleres Arbeiten, erhöht aber gleichzeitig den Bedrohungsfaktor erheblich.

Auch die Datenmenge, mit der Mitarbeiter außerhalb des Büros arbeiten, erhöht sich durch das Wachstum des Internets der Dinge (Internet of Things, IoT) rasant. Damit verbunden nehmen die Erfassung, Speicherung und Verarbeitung der Daten ganz neue Dimensionen an. Unternehmen setzen vermehrt auf Edge-Computing-Modelle, bei denen immer leistungsfähigere Geräte die Daten lokal verarbeiten, anstatt sie an externe Server zu senden. Dies reduziert zwar die Datenmengen, die in einer zentralen Cloud verarbeitet werden müssen, stellt jedoch immer noch eine erhebliche Herausforderung für die IT-Abteilung dar.

Eine Studie von Bitglass hat gezeigt, dass verlorene oder gestohlene Geräte die Hauptursache von Datenschutzverletzungen sind und für mehr als ein Viertel der Vorfälle verantwortlich waren, bei denen Informationen in falsche Hände geraten sind.

Sicherheit für mobile Mitarbeiter: **Risiken**

Mit dem zunehmenden Trend der mobilen Arbeit sind auch eine Reihe an Sicherheitsrisiken verbunden, die Unternehmen vor neue Herausforderungen stellen. Von verloren gegangenen Notebooks über die Nutzung von Cloud-Diensten außerhalb des Unternehmens bis hin zur Gefahr physischer Manipulationen an der Unternehmenshardware durch Kriminelle und Firmenspione – die Liste potenzieller Gefahren ist lang. Deshalb ist es für Unternehmen das A&O, die Sicherheit ihrer Remote-Mitarbeiter ganzheitlich zu betrachten und ein entsprechendes Sicherheitskonzept zu entwickeln.

Das Konzept der „Perimeter Sicherheit" ist traditionell für die meisten IT-Abteilungen von entscheidender Bedeutung: Perimeter-Firewalls am Rande der Unternehmensnetzwerke schützen die Daten, die sich innerhalb der Netzwerke befinden, vor Angriffen. Die Zunahme des mobilen Arbeitens allerdings bringt dieses Konzept an seine Grenzen: Cloud-Services, mobiles Arbeiten und die verstärkte Zusammenarbeit innerhalb von Organisationen lassen es praktisch bedeutungslos werden.

Das unmittelbarste Risiko ist die Tatsache, dass das Gerät mobil ist. Trotz dessen, dass beispielsweise Notebooks sensible persönliche Daten enthalten, passiert es zudem nicht selten, dass Nutzer ihr Gerät verlieren und zum Beispiel auf dem Rücksitz eines Taxis oder im Gepäckraum des Flugzeugs liegen lassen. Allein im Jahr 2017 wurden beispielsweise über 34.000 Smartphones und rund 1.000 Notebooks als Fundsachen bei den Londoner Verkehrsbetrieben abgegeben.

Eine Studie von Bitglass hat gezeigt, dass verlorene oder gestohlene Geräte die Hauptursache von Datenschutzverletzungen sind und für mehr als ein Viertel der Vorfälle verantwortlich waren, bei denen Informationen in falsche Hände geraten sind. Hackerangriffe oder Sicherheitsverstöße von Mitarbeitern zählten deutlich seltener zu den Gründen für Verletzungen des Datenschutzes.

Sicherheit für mobile Mitarbeiter: **Auswirkungen**

Diese vielen Risikofaktoren des modernen mobilen Arbeitens haben gravierende Auswirkungen. Das beginnt damit, dass bei fehlenden oder beschädigten Geräten die Produktivität leidet und Kosten für Ersatzgeräte entstehen. Hinzu kommen die Gefahren, die mit dem physischen Zugriff auf einen Firmenrechner verbunden sind – und diese könnten noch deutlich schlimmere Folgen haben.

Auch das Risiko der Wirtschaftsspionage spielt hierbei eine Rolle. Leider sind die Taktiken, die man im Allgemeinen aus der Welt der Wirtschaftsspione kennt, heute auch für andere Personen verfügbar, solange diese ausreichend Geld für deren Beschaffung aufbringen können. Wenn ein Computer oder eine Software eine Schwachstelle aufweist, kann es durchaus sein, dass der erste, der diesen Fehler entdeckt, ein Hacker ist und diese Informationen umgehend an den Höchstbietenden verkauft. Das kann ein staatlicher Geheimdienst, eine organisierte kriminelle Bande oder irgendjemand sein, der unlautere Geschäfte für Unternehmen abwickelt, die selbst eine weiße Weste behalten möchten.

Verschärft wird diese Situation noch durch den jüngsten Trend der Sicherheitsagenturen, die ihr Wissen häufig über nicht gepatchte Sicherheitslücken geheim halten und dann selbst gehackt werden. Als mehrere Ransomware-Angriffe im Jahr 2017 weltweit Panik und Schäden verursachten, wurden Tools verwendet, die über eine große Sicherheitslücke bei der US National Security Agency entwendet wurden.

„Edge-Computing“, also der Schutz der Peripherie, bietet umfassende Möglichkeiten, Unternehmensnetzwerke vor Malware zu schützen, indem es die Daten am Rande des Netzwerks bereit hält. Diese Daten müssen jedoch sicher aufbewahrt werden. Dies wird umso wichtiger, wenn man bedenkt, welche Arten von Daten das Internet der Dinge (Internet of Things, IoT) in sensiblen Bereichen wie dem Gesundheitswesen oder dem Verkehr erzeugt. Sobald Menschen betroffen sind, können Datenschutzverletzungen fatale Folgen nach sich ziehen.

Die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union, die im Mai 2018 in Kraft getreten ist, enthält strenge Anforderungen an Unternehmen, bei denen Sicherheitsverletzungen in Bezug auf personenbezogene Daten auftreten. Sollte es zu einem Verstoß kommen, muss das Unternehmen die zuständige Datenschutzbehörde innerhalb von 72 Stunden benachrichtigen. Dabei müssen unter anderem auch die Maßnahmen angeben werden, die ergriffen wurden, um den Verstoß zu beheben und die möglichen schädlichen Auswirkungen zu mildern.

Führt der Verstoß zu einer Geldbuße, kann diese durch einen Nachweis umfassender Investitionen in die Sicherheit reduziert werden. Wie es in Artikel 34 der DSGVO heißt, ist es nicht erforderlich, Einzelpersonen über den Vorfall zu informieren, wenn das Unternehmen „geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden“. Angesichts von drohenden DSGVO-Bußgeldern in Höhe von bis zu vier Prozent des weltweiten Umsatzes oder 20 Millionen Euro, je nachdem, welcher Betrag höher ist, waren angemessene Sicherheitsmaßnahmen nie wichtiger als heute.

Edge-Computing“, also der Schutz der Peripherie, bietet umfassende Möglichkeiten, Unternehmensnetzwerke vor Malware zu schützen, indem es die Daten am Rande des Netzwerks bereit hält. Diese Daten müssen jedoch sicher aufbewahrt werden. Dies wird umso wichtiger, wenn man bedenkt, welche Arten von Daten das Internet der Dinge (Internet of Things, IoT) in sensiblen Bereichen wie dem Gesundheitswesen oder dem Verkehr erzeugt.

Sicherheit für mobile Mitarbeiter: **Lösungen**

Die Abwehr von Sicherheitsbedrohungen im mobilen Arbeitsumfeld beginnt mit der Tatsache, dass der Mensch das schwächste Glied in der Kette ist: Nicht selten lassen Nutzer Dinge herumliegen, wo sie nicht liegen sollten, oder sie nutzen Anwendungen, die sie besser vermeiden sollten. Ein weiterer wichtiger Punkt: Viele Anwender wählen schwache Kennwörter für ihre mobilen Geräte und sie benutzen öffentliche WLAN-Hotspots, die unzureichend gesichert sind.

Um das Unternehmen und eines seiner wertvollsten Güter, die unternehmenskritischen Daten, umfassend zu schützen, ist eine Reihe an Sicherheitsmaßnahmen notwendig. Diese Maßnahmen bedürfen zwar einerseits einer umfangreichen und detaillierten Planung. Andererseits tragen sie aber einen entscheidenden Teil dazu bei, das Angriffsrisiko eines Unternehmens erheblich zu verringern sowie seine Fähigkeit zu verbessern, im Falle einer Bedrohung entsprechend reagieren zu können.

Schulung der Mitarbeiter

Allem voran müssen IT-Abteilungen sicherstellen, dass ihre Mitarbeiter in puncto Datensicherheit beim mobilen Arbeiten umfassend geschult werden. Die Mitarbeiter sollten die Prinzipien starker Kennwörter und verschiedener Verschlüsselungstools verstehen, mit denen sie – und auch die Unternehmensdaten – sicher sind. Die meisten Menschen halten ihre Geräte so leicht zugänglich wie möglich. Lange, komplizierte Kennwörter, die den Unternehmensrichtlinien entsprechen, erschweren dies natürlich. Deshalb sollte den Mitarbeitern gezeigt werden, wie Virtual Private Networks (VPNs) verwendet werden können, um einen sicheren Zugriff auf Unternehmensdaten und services zu gewährleisten – speziell wenn sie über Verbindungen auf den Firmenserver zugreifen, die potenziell unsicher sein könnten, wie zum Beispiel öffentliche Hotspots.

Diese Sicherheitsschulungen sollten nicht nur ein Mal erfolgen, sondern das Wissen der Mitabeiter hinsichtlich der Datensicherheit muss kontinuierlich aufgefrischt werden. Über die Hälfte der Verstöße beginnt mit einem Phishing-Angriff. Deshalb ist es zudem wichtig, dass die Mitarbeiter auch geschult werden um solche offensichtlichen Methoden rechtzeitig zu erkennen. Dies sind oft einfache Dinge, wie die Suche nach einer URL für https:// oder das Auffinden ungewöhnlicher URL-Endungen bei Websites (.pl statt .com). Die Methoden entwickeln sich jedoch so schnell weiter, dass es auch in diesem Bereich essenziell ist, die Mitarbeiter kontinuierlich zu schulen und über die neuesten Bedrohungen auf dem Laufenden zu halten, ob es sich um neue Ransomware handelt, die die Runde macht, oder um neue Techniken, mit denen Angreifer potenzielle Schwachstellen des Nutzers selbst oder der Technik ausnutzen.

Insbesondere mobile Mitarbeiter sollten sich der Gefahren von Hacker-Angriffen oder des Ausspähens von Daten zum Beispiel durch einen beiläufigen Blick einer fremden Person über die Schulter bewusst sein – gerade in Zügen, Cafés oder gemeinsam genutzten Arbeitsräumen ist es kinderleicht, einen Blick auf den Bildschirm einer anderen Person zu werfen. In Sekundenschnelle hat derjenige Zugang zu wertvollen Informationen. Um dagegen zu wirken, kann das Unternehmen zwar Datenschutzfilter bereitstellen. Aber der eigentliche Schlüssel zu mehr Sicherheit sind in diesem Fall die Aufmerksamkeit und das Verantwortungsgefühl des Nutzers.

Ein mobiler Mitarbeiter, der in einem Café oder einer Flughafen-Lounge sitzt und auf Netzanbindung angewiesen ist, wird immer versucht sein, den nächstgelegenen öffentlichen Hotspot zu nutzen. Für Kriminelle ist es sehr einfach, gefälschte Hotspots einzurichten, die das Aussehen einer echten Verbindung vortäuschen. Einmal angemeldet, bieten diese Access Points eine hervorragende Möglichkeit, Daten abzufangen. Um dem Mitarbeiter ein Gefühl dafür zu vermitteln, wo mögliche Angriffe lauern können und wo sie zum Beispiel über ein öffentliches WLAN in Gefahr geraten können, sind regelmäßige Schulungen ebenfalls von essenzieller Bedeutung.

Sicherheitsbedrohungen entwickeln sich ständig weiter. Daher sollten die Sicherheitskonzepte der Unternehmen und das Bewusstsein der Mitarbeiter stets auf dem neuesten Stand sein. Für IT-Mitarbeiter besteht die größte Herausforderung darin, ein ausgewogenes Verhältnis zwischen ihrer Rolle als IT-Helfer in der täglichen Arbeit einerseits und als Beschützer vor möglichen Sicherheitsbedrohungen andererseits zu finden. Zu häufige Sicherheitsschulungen werden schnell von der Belegschaft ignoriert, zu wenige lassen wiederum das Verantwortungsgefühl schwinden. Das Engagement der Mitarbeiter ist allerdings essenziell, um eine starke Sicherheitskultur innerhalb des Unternehmens zu schaffen. Eine klare Definition von möglichen Risiken und damit verbundenen Verantwortlichkeiten trägt einen wichtigen Teil dazu bei, die Sicherheit im Unternehmen umfassend zu gewährleisten.

IT-Governance

Eine sehr gute IT-Governance trägt einen wichtigen Teil zu einem verbesserten Datenschutz im Unternehmen bei. So sollte eine Organisation sicherstellen, dass ihre Prozesse eine umfassende Sicherheitstrategie mit einschließen – gerade vor dem Hintergrund der vielfältigen Risiken, die das mobile Arbeiten mit sich bringt. Regelmäßige Überprüfungen der Berechtigungen sind beispielsweise in diesem Zusammenhang unerlässlich, um unerlaubte Zugriffe zu verhindern. Auch sollte jedes Unternehmen eine Strategie definiert haben, wie mit dem Austritt von Mitarbeitern umgegangen wird, um beispielsweise deren weiteren Zugriff auf das Unternehmensnetzwerk deaktivieren zu können.

Mobile Endgeräte werden zunehmend wichtige Faktoren für die IT-Governance im Bereich der mobilen Sicherheit. Neben einer Vielzahl von preiswerten mobilen Endgeräten, die für geschäftliche Zwecke eingesetzt werden, kommt heute auch eine stark wachsende Zahl von IoT-Geräten hinzu, für die klare Datenschutz- und Sicherheitsrichtlinien ebenfalls unabdingbar sind.

Die Nutzung unterschiedlicher Geräte und Cloud-Dienste durch die Mitarbeiter muss genauestens koordiniert und überwacht werden, damit die IT-Mitarbeiter exakt wissen, welcher Mitarbeiter über welche Geräte verfügt und welche Services nutzt. Zudem erweisen sich entsprechende Tools als essenziell, um den Sicherheits- und Datenrichtlinien des Unternehmens umfassend Rechnung zu tragen.

Die Nutzung unterschiedlicher Geräte und Cloud-Dienste durch die Mitarbeiter muss genauestens koordiniert und überwacht werden, damit die IT-Mitarbeiter exakt wissen, welcher Mitarbeiter über welche Geräte verfügt und welche Services nutzt. Zudem erweisen sich entsprechende Tools als essenziell, um den Sicherheits- und Datenrichtlinien des Unternehmens umfassend Rechnung zu tragen.

Software und Hardware

Hinsichtlich der Hard- und Software im mobilen Arbeitsumfeld lassen sich zwei Hauptbereiche ausmachen: die Verwaltung der mobilen Geräte sowie Virtualisierungssoftware.

Softwarepakete für die Verwaltung von Mobilgeräten sind unerlässlich. Damit werden die Geräte nicht nur mit den aktuellsten Sicherheitseinstellungen auf dem neuesten Stand gehalten. Vielmehr wird darüber auch gewährleistet, dass die mobilen Geräte den Unternehmenrichtlinien entsprechen, wie zum Beispiel über die strikte Trennung von persönlichen und Unternehmensdaten auf einem Gerät, das für geschäftliche wie auch private Zwecke verwendet wird.

Einige Unternehmen bevorzugen auch Virtualisierungssoftware, die es ihren Mitarbeitern ermöglicht, bestimmte Aufgaben über einen virtuellen Desktop zu erledigen, ohne dass Daten lokal gespeichert werden müssen. Mobile Zero Client-Lösungen ermöglichen den Einsatz von Computern, die weder über ein Betriebssystem noch über eine Festplatte verfügen. So wird das Risiko von Diebstahl oder dem Aufspielen von Malware auf ein Minimum reduziert.

Eine gute Auswahl der Hardware ist zudem ein entscheidender Faktor, um das mobile Arbeiten sicher zu gestalten. So sollten Unternehmen für ihre Mitarbeiter Notebooks einsetzen, die besonders widerstandsfähig sind und dem rauen Geschäftsalltag standhalten können. Geräte mit H.A.L.T. (Highly Accelerated Life Testing) Zertifizierung entsprechend des TÜV Rheinlands zum Beispiel erfüllen diese Anforderungen und gewährleisten eine maximale Robustheit. Zudem sollten die Notebooks Stürze, Verbiegungen oder auch das Verschütten kleinerer Mengen an Flüssigkein problemlos überstehen können.

Am sichersten sind Notebooks von PC-Herstellern, die ihr eigenes BIOS schreiben, das niemand manipulieren kann. Ein Hersteller sollte zudem eine umfassende Verschlüsselung anbieten. Diese muss dafür Sorge tragen, dass die Systemdateien, das Betriebssystem und die per E-Mail und USB weiter verbreiteten Dateien geschützt werden und diesen verschlüsselten Status im Idealfall beibehalten, selbst wenn jemand die Festplatte des Computers entfernt.
Ebenso ist es sinnvoll, dass die Notebooks der Mitarbeiter über neueste biometrische Authentifizierungsverfahren verfügen, um sicherzustellen, dass nur die richtigen Personen Zugang zum Rechner erhalten. Zu den biometrischen Technologien zählen zum Beispiel Touchpads mit integrierten Fingerabdruckscannern oder die Authentifizierung über die Gesichtserkennung.

Zwar gibt es keinen Königsweg für sicheres mobiles Arbeiten, der für alle Unternehmen gleich sinnvoll ist. Denn die maximale Sicherheit im mobilen Geschäfsalltag kann nur ein individuelles, auf das Unternehmen zugeschnittene Sicherheitskonzept gewährleisten. Aber was für alle Organisationen gilt: Ein ganzheitlicher Sicherheits-ansatz, der die Schulung der Mitarbeiter, sinnvolle Sicherheits-richtlinien sowie sichere Soft- und Hardware berücksichtigt, stellt die Grundvorausetzung für ein professionelles mobiles Arbeitsumfeld sicher.

Kosten für verlorene Geräte und Daten:

- Eine Studie von Kensington zeigte, dass alle 53 Sekunden ein Notebook gestohlen wird und dass 4,3 Prozent der Unternehmens-Smartphones jährlich geklaut werden oder verloren gehen.
- Sie zeigte auch, dass 80 Prozent der Kosten bei gestohlenen Notebooks auf den damit verbundenen Datenverlust zurückzuführen sind.
- Der Produktivitätsverlust sowie der Zeit- und Kostenaufwand für die Bereitstellung eines Ersatzgerätes sind ebenfalls zu berücksichtigen.
- Datenschutzverletzungen können schwerwiegende Folgen durch Rufschädigung sowie erhebliche finanzielle Probleme nach sich ziehen.
- Wenn Daten in die Hände von Wettbewerbern fallen, können die strategischen Kosten für das Unternehmen unkalkulierbar sein.

Vorteile des dynabook Mobile Zero Client (dMZC):

- Der dMZC ist auf Basis verschiedener Business-Notebooks von dynabook erhältlich.
- Der dMZC benötigt kein Betriebssystem und keine Festplatte, sodass die Mitarbeiter sensible Daten ausschließlich über einen virtuellen Desktop bearbeiten können.
- Der dMZC unterstützt die wichtigsten cloudbasierten Virtual-Desktop-Infrastrukturlösungen einschließlich Citrix und VMware, ist aber auch nicht ausschließlich mit diesen kompatibel.
- Mitarbeiter können den dMZC über 4G oder über jede Internetverbindung nutzen.
- Ohne die Notwendigkeit lokal gespeicherter Daten reduziert der dMZC das Risiko von Maleware und Gerätediebstahl auf ein Minimum.

DSGVO-Implikationen und -Bußgelder:

- Seit die DSGVO im Mai 2018 in Kraft getreten ist, werden Organisationen, die Verstöße gegen personenbezogene Daten erlitten haben, dazu verpflichtet, Regulatoren und potenziell auch ihre Kunden davon in Kenntnis zu setzen.
- Diese Veröffentlichung dürfte in einigen Fällen zu einer Rufschädigung führen.
- Wenn ein Datenverarbeitungsverantwortlicher seine Sicherheitspraktiken nicht nachhaltig genug umsetzt, kann dies zu Geldbußen in Höhe von 20 Millionen Euro oder vier Prozent des weltweiten Jahresumsatzes des Unternehmens führen, je nachdem, welcher Betrag höher ist.

Portégé X30-F & Tecra X40-F-Serie:

- Sicheres Einloggen mit der biometrischen Gesichts-erkennung über Windows Hello oder Intel® Authenticate.
- Höchste Sicherheit durch dynabook's eigen entwickeltes BIOS. Daher hat kein Drittanbieter Zugang zum BIOS, was höchste Sicherheitsstandards ermöglicht.
- TPM 2.0 Verschlüsselung und je nach Modell mit integriertem Fingerabdrucksensor.
- Weitere Sicherheit bietet der optionale Smartcard Reader.
- Ihre Daten sind leicht zugänglich für Sie, aber fast unzugänglich für die falschen Hände.

Weitere Informationen über neueste Trends und Lösungen von dynabook sind auf dem Blog Toshibytes erhältlich. www.toshiba.de/Toshibytes

Unser Vertriebsteam erreichen Sie über diese E-Mail-Adresse: DACH.contact@dynabook.com

dynabook