Überblick zur aktuellen IT-Bedrohungslage

Im Fadenkreuz

von Thomas Gronenwald

Unternehmen stehen zunehmend im Fokus von Cyberangriffen. So erwarten IT-Sicherheitsexperten auch künftig eine steigende Anzahl zielgerichteter Attacken. Jede noch so kleine Schwachstelle wird dabei ausgenutzt und in der Regel stehen finanzielle, manchmal auch politische Absichten hinter solchen Angriffen. Neben zahlreichen Lücken in der Software stellen die Mitarbeiter selbst einen entscheidenden Schwachpunkt dar. Wo die Gefahren lauern und wie Sie Ihre IT-Umgebung schützen, lesen Sie in diesem Beitrag.

In den vergangenen zwei Jahren haben zielgerichtete Attacken, sogenannte "Targeted Attacks", gegen Unternehmen stark zugenommen und dürften auch weiterhin steigen. Organisationen werden sich in diesem Zusammenhang vermehrt mit dem Thema Cyber-Spionage auseinandersetzen müssen. Auch die Betreiber kritischer Infrastrukturen verzeichnen häufiger Angriffe auf ihre kritischen Industrieanlagen und müssen daher spezielle Sicherheitsvorkehrungen treffen.

Dabei dürften neuartige Cyberangriffe, wie wir sie beispielsweise mit "Flame" erlebt haben, einen neuen Höchststand erreichen. Flame war das bis dato größte und anspruchsvollste Cyberspionageprogramm, das öffentlich bekannt wurde. Nach Expertenmeinung existierte Flame bereits seit mindestens fünf Jahren. Innerhalb dieses Zeitraums wurden mit diesem Schadcode über einen langen Zeitraum unvorstellbare Mengen von sensiblen Daten gesammelt. Weiterhin lässt sich ein Anstieg auf Java-Schwachstellen auf PCs feststellen. Erfreulich hingegen ist zumindest der Rückgang von Angriffen auf Adobe Flash und Adobe Reader. Hier konnte der Hersteller mittels automatisierter und funktionierender Update-Mechanismen dem Trend entgegenwirken. Nichtsdestotrotz stehen neben Java weiterhin Adobe Flash und Adobe Reader ganz weit vorne auf der Angriffsliste von Cyber-Kriminellen.

Gezielte Angriffe

In den letzten Jahren verzeichnete die Industrie zahlreiche Hacker-Angriffe. Die Dunkelziffer hierbei liegt aller Voraussicht nach wesentlich höher. Zu den bekanntesten Angriffen gehörte der Einbruch beim japanischen Elektronikkonzern Sony und dessen Sony Entertainment Network, des Playstation Network und Sony Online Entertainment. Als Ergebnis sollen laut Experten rund 100 Millionen gestohlene Kundendatensätze gestanden haben. Sony ist dabei nur ein prominentes Beispiel. Auch Neckermann, Sega oder RSA wurden Opfer großangelegter Angriffe.

Auch in Deutschland sind Netzwerke nicht vor Attacken sicher. Im Februar wurde der erfolgreiche Angriff auf die Webseite sparkasse.de bekannt. Dort hatten Angreifer auf mehreren Unterseiten Malware platziert. Im März 2013 lief zudem eine DDoS-Attacke (Distributed Denial of Service) gegen die Anti-Spam-Organisation Spamhaus. Dieser enorme und datenintensive Angriff, den das Bundesamt für Sicherheit in der Informationstechnik (BSI), als "massivsten seiner Art" bezeichnete, verlangsamte sogar die Internetgeschwindigkeit weltweit.

Profil der Angriffe

Das Profil der Angriffe zeugt vermehrt von Zielen mit wirtschaftlichem und politischem Hintergrund. Die Angreifer sind dabei weltweit organisiert und scheinbar mit einem enorm hohen finanziellen Background ausgestattet. Auffällig dabei ist, dass das Vorgehen der Angreifer zumeist auf einem gewissen Schema basiert:

- Ausnutzen von eher unbekannten Schwachstellen
- Angriffe über einen sehr langen Zeitraum hinweg
- Erster Schritt ist oft die Übernahme eines Internetservers oder Versand von Malware
- Nächster Schritt ist dann ein Angriff des internen Netzwerkes

Social Engineering

Alle technischen Sicherheitsmaßnahmen gegen das Ausspionieren von Firmeninformationen helfen nichts, wenn der Mensch

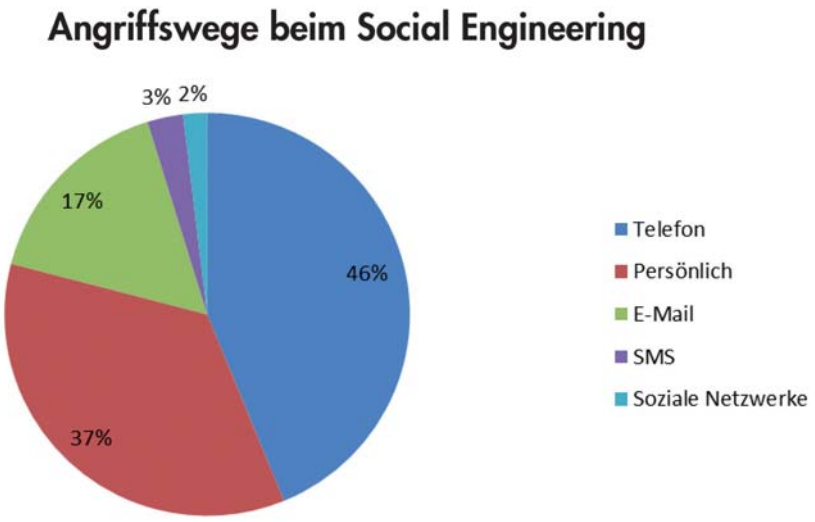

Bild 1: Telefonanrufe und persönliche Treffen stehen beim Social Engineering hoch im Kurs

nicht sensibilisiert ist. Der Mitarbeiter bildet die Sicherheitslücke schlechthin – daher ist Social Engineering eine der erfolgreichsten Angriffsmethoden. Als Social Engineering werden Attacken bezeichnet, die nicht auf einen Computer, sondern auf dessen Benutzer gerichtet sind. Hierbei versucht ein Angreifer, vertrauliche Informationen wie Login-Daten oder Passwörter auszuspähen. Der Erstkontakt erfolgt dabei in der Regel per E-Mail, Telefon oder durch ein persönliches, inszeniertes Treffen. Aber auch die Nutzung von sozialen Netzwerken wie Facebook oder LinkedIn mit dem Ziel, sensible Informationen über eine Zielperson zu erhalten, stehen hoch im Kurs.

Die Angreifer nutzen menschliche Eigenschaften wie Hilfsbereitschaft, Kundenfreundlichkeit, Dankbarkeit, Stolz, Gutgläubigkeit, Respekt, Bestechlichkeit, Konfliktvermeidung oder auch ein einfaches Liebesbedürfnis aus. Je nach Opfer werden in der Praxis die erfolgreichsten psychologischen Methoden und Tricks ausgewählt. Ein Angriff läuft in der Regel anhand folgender psychologischer Tricks ab:

- Neugier: Neugierde ist eine durchaus positive Eigenschaft, die es uns Menschen erlaubt, Neues zu erlernen und neue Erfahrungen zu gewinnen. Aber unsere Neugier kann ebenso eine erhebliche Gefahr darstellen. Malware verbreitet sich oft dadurch, dass Anwender eine E-Mail mit einem Anhang zugesandt bekommen, der scheinbar etwas enthält, was ihre Neugierde weckt und sie dazu bringt, den Anhang zu öffnen.
- Belohnungen: Gewinne, Steuerrückzahlungen oder andere finanzielle Vorteile zu versprechen, ist ein beliebtes psychologisches Mittel, um an Informationen wie Bankverbindungen oder Kreditkartendaten zu kommen.
- Angst: Oft versuchen Angreifer auch, ihre Opfer dazu zu bewegen, etwas zu tun, etwa eine Datei zu öffnen, indem sie ihnen Angst machen. Auch dieses Prinzip findet sich meistens bei der Verbreitung von Schadsoftware wieder. Die E-Mail enthält dann beispielsweise die Behauptung, man habe eine Rechnung über mehrere tausend Euro zu zahlen oder sei angezeigt worden.
- Hilfsbereitschaft: Oftmals wird von Angreifern auch an das Gewissen oder die Hilfsbereitschaft ihrer Opfer appelliert. In E-Mails wird dann behauptet, ein Anhang, der in Wahrheit wiederum einen Schädling enthält, enthalte Informationen, wie man Opfern einer humanitären Katastrophe oder auch einzelnen Menschen, die angeblich ein schweres Schicksal haben, helfen könne.
- Autorität: Ein Angreifer gibt sich dabei in der Regel als Autoritätsperson aus, um Account-Informationen zu erlangen. Meist kommt zum autoritären Auftreten noch das Spiel mit der Angst.

Mobile Plattformen im Fokus

Wie es scheint, haben Cyber-Kriminelle inzwischen auch Geschmack an mobiler Malware gefunden. Nachdem es im Jahr 2012 einen regelrechten Boom gab, ging es 2013 genauso weiter. Dabei konzentrieren sich die Entwickler vermehrt auf das beliebte Betriebssystem Android und entwickeln vor allem Drive-by-Download-Angriffe. Mittels manipulierter Webseiten werden die Benutzer beim Surfen im Web unbemerkt infiziert. Der Grund dafür sind nicht gepatchte Schwachstellen im Betriebssystem oder einer installierten App. Ziel ist es unter anderem, an die Daten auf Smartphones und Tablets heranzukommen. Für Unternehmen wie auch Anwender kein schönes Szenario.

Der bis dato raffinierteste mobile Trojaner wurde im zweiten Quartal 2013 entdeckt. Der Schadcode mit Namen "Backdoor.AndroidOS.Obad.a" nutzte drei bisher unveröffentlichte Sicherheitslücken aus. Er kann SMS-Nachrichten versenden, andere Schadprogramme laden, installieren und diese via Bluetooth versenden sowie Remotebefehle von der Kommandozeile ausführen. Die Entwickler nutzten dazu eine bis dato unbekannte Sicherheitslücke in Android, die es ermöglicht, erweiterte Admin-Rechte zu erhalten, ohne in der Liste der Anwendungen mit diesen Privilegien aufgeführt zu werden. So ist es quasi unmöglich, die Malware von dem mobilen Gerät zu entfernen. Die erweiterten Rechte können von dem Trojaner ebenso genutzt werden, um den Bildschirm des Gerätes kurzfristig zu blockieren. Dies geschieht typischerweise nach der Verbindung zu einem freien WLAN, das vom Schädling genutzt wird, um sich selbst oder andere schädliche Anwendungen an Geräte in der Nähe zu versenden. Nach dem Erststart trägt die Malware einige Informationen zusammen, unter anderem die folgenden:

- MAC-Adresse
- Netzbetreibernamen
- Telefonnummer
- IMEI
- Kontostand
- Ortszeit
- Informationen über Administrator-/Root-Berechtigungen

Alle diese Daten werden an den Command & Control-Server gesendet. Um die Informationen über ein infiziertes Gerät und seine Funktion zu versenden, nutzt Backdoor.AndroidOS.Obad.a die aktuell aktive Internetverbindung. Ist keine Verbindung verfügbar, sucht der Trojaner nach WLANs in der Nähe, die keine Authen-

tifizierung erfordern und verbindet sich mit einem der gefundenen Netzwerke. Die Entwickler sind zudem in der Lage, den Trojaner mit Hilfe von Textnachrichten zu kontrollieren. Dies war bislang im Bereich von mobilen Geräten und mobiler Malware einmalig und verdeutlicht das Potenzial für Cyber-Kriminelle.

Unternehmen sind daher gefordert, Ihre Sicherheitsmaßnahmen laufend zu überprüfen und entsprechend der Bedrohungslage anzupassen. Speziell die Bereiche der mobilen Sicherheit und die Themen rund um das Patch-Management von Applikationen und Apps spielen eine immer größer werdende Rolle.

Bedrohungen durch Spam

Rund 90 bis 95 Prozent der weltweit versendeten E-Mails sind unerwünscht und somit Spam. Im April 2013 blieb das Führungsduo der Länder, die weltweit am meisten Spam versenden, unverändert: An erster Stelle steht dabei erneut China (23,9 Prozent), obwohl dessen Anteil um fast zwei Prozentpunkte zurückging. Der aus den USA stammende Spam-Anteil ging geringfügig auf 16,8 Prozent zurück – somit stammten etwa 41 Prozent des weltweiten Spam-Aufkommens aus diesen beiden Ländern.

Die Bedrohungslage im Bereich von E-Mails ist in den vergangenen Jahren stetig gestiegen. Obwohl ein genereller Rückgang von Spam-Nachrichten festgestellt werden konnte, steigt der Anteil gefährlicher E-Mails deutlich. Der Anteil besonders gefährlicher E-Mails wie Malware-Nachrichten, Drive-by-Angriffe und gezielte Phishing E-Mails ist demnach stark angewachsen und wird zunehmend zielgerichtet und präzise an ausgewählte Empfänger verschickt. Immer häufiger ist dabei zu beobachten, dass aktuelle Großereignisse zu Spamwellen führen. So beispielsweise Sportereignisse wie die Olympischen Spiele oder Welt- und Europameisterschaften, die in der Regel zu neuen Spamwellen führen.

Daten abgeschöpft mit Phishing

Angreifer und Datendiebe nutzen Spam-E-Mails, gefälschte Webseiten oder E-Mail- sowie Instant Messaging-Nachrichten, um andere Benutzer zur Herausgabe vertraulicher Informationen zu verleiten, beispielsweise Einzelheiten zu Bank- und Kreditkartenkonten. Oft wird hierbei versucht, unter einem bestimmten Vorwand wie beispielsweise einer bevorstehenden Girokonto-Sperrung, unvorsichtige Anwender in die Falle zu locken.

Der Angreifer versucht dabei immer mit Tricks, den Benutzer dazu zu verleiten, einen ihm übermittelten Anhang zu öffnen. Tut er dies, wird automatisch Malware auf den Computer des Benutzers geladen. Ihre Mitarbeiter sollten daher peinlichst genau darauf achten, keine unbekannten Anhänge zu öffnen – insbesondere, wenn Sie den Absender nicht genau kennen. Dies gilt im Übrigen auch für die Ergebnisse einer Suchanfrage. Dateien sollten in den vorgeschlagenen Suchergebnissen keinesfalls geöffnet werden, sofern sie nicht eindeutig als sicher identifiziert werden können. Hilfreich dabei sind Tools, die bei der Bewertung der Websites unterstützen, sogenannte Reputationsdienste, und den Nutzern mitteilen, ob die Seite vertrauenswürdig ist oder nicht. Ein Beispiel hierfür ist das kostenlose Firefox Add-on "WOT".

Nicht immer enthalten Spam-Mails einen infizierten Anhang. Vielmehr versuchen Malware-Versender, ihren Schadcode in der E-Mail zu verlinken. Dabei versehen die Angreifer und Entwickler die E-Mail mit einem Link zu einer manipulierten Website, in der Hoffnung, dass viele Nutzer eher einen Link anklicken als ein Attachment zu öffnen. Die verlinkten Seiten sind so manipuliert, dass dem Nutzer allein durch den Besuch der Website per Drive-by-Download die Schadsoftware untergeschoben wird. Wird diese im Browser geöffnet, erfolgt eine automatische Infektion über bekannte Sicherheitslücken im Browser. Auch hier sollten Nutzer keinesfalls den Anweisungen innerhalb der nichtvertrauenswürdigen E-Mail folgen.

Drive-by-Spam

Noch arglistiger ist eine Methode, die in letzter Zeit häufiger Anwendung findet. Dabei wird eine HTML-Seite in eine E-Mail eingebettet. Diese HTML-Datei ist in der Regel mit einem JavaScript versehen, das automatisch Malware herunterlädt. Hierfür genügt es bereits, die E-Mail nur zu öffnen. Ein Klicken auf einen Link oder das Öffnen eines Anhang entfällt somit. Populäre E-Mail-Programme wie Outlook haben bereits seit längerem auf diese Sicherheitsanfälligkeit reagiert und JavaScript deaktiviert. Sie sollten trotzdem überprüfen, ob die Mail-Clients in Ihrem Unternehmen JavaScript nutzt oder nicht.

Wirkungsvolle Schutzmaßnahmen

Eine grundlegende Sicherheitsmaßnahme ist das fortwährende Aktualisieren von Software. Dafür sollten Sie zeitnah für alle installierten Anwendungen inklusive dem Betriebssystem die veröffentlichten Updates und Sicherheitsupdates installieren. Hervorzuheben sind dabei Sicherheitsupdates für die eingesetzten Browser wie Internet Explorer, Firefox oder Chrome sowie den Adobe Flash Player und Acrobat Reader sowie alle installierten Java-Versionen. Im Unternehmen stellt sich dies jedoch in der Regel als durchaus schwierige Aufgabe dar.

Patch-Management

Etabliert hat sich mittlerweile das zyklische Aktualisieren von Windows selbst. In der Regel findet dies einmal monatlich, idealerweise nach einem Test für eine repräsentative Gruppe von Systemen im Unternehmen statt. Microsoft hat hierfür über mehrere Jahre hinweg gut funktionierende Lösungen wie Microsoft-Update, WSUS oder System Center entwickelt, über die sich die veröffentlichten Updates in der Regel ohne Probleme installieren und überwachen lassen. Nicht nur aus diesem Grund bewegt sich die Gefährdungslage in Richtung der installierten Anwendungen, sprich: den Third-Party-Applikationen.

Die Entwickler von Schadcode haben die Verbreitung dieser Applikationen erkannt und entwickeln tagtäglich neue Malware. Aufgrund der oft mäßigen Update-Methoden der Hersteller haben die Entwickler mehr Zeit bis zum Schließen der Sicherheitslücke und dem Verteilen der Updates durch den Hersteller. Einige Security-Anbieter wie Secunia oder Lumension bieten zum Management und zur Aktualisierung von Anwendungen spezielle Produkte an. Hiermit ist sowohl eine Überwachung der

eigenen Infrastruktur als auch ein zeitnahes Patchen der im Einsatz befindlichen Applikationen möglich. Bei der Aktualisierung von Anwendungen spielt der Zeitfaktor eine nicht unwesentliche Rolle. Durch bereits fertig konfigurierte Update-Pakete, die innerhalb des Applikations-Pools zum Download bereitstehen, können Tests schnell durchgeführt werden und aufgetretene Schwachstellen zeitnah beseitigt werden. Hierbei entfällt das langwierige Erstellen von Update-Paketen und aufwändiges Testen.

Angriffsfläche reduzieren

Reduzieren Sie die Angriffsfläche Ihrer Systeme, indem Sie sich auf die nötigsten Anwendungen konzentrieren: Installieren Sie nur Applikationen, die Sie auch wirklich benötigen und deinstallieren Sie solche, die Sie nicht mehr brauchen. Dies verringert nicht nur die Angriffsvektoren sondern auch den Aktualisierungsaufwand Ihrer Systeme. Zusätzlich sollten Sie Ihre Systeme einer grundsätzlichen Härtung unterziehen. Deaktivieren Sie nicht benötigte Dienste – zur Unterstützung erweist sich hierzu der Microsoft Security Compliance Manager als hilfreich. Mit diesem ist es möglich, die Angriffsfläche zu bewerten und geeignete Gruppenrichtlinien zu definieren und umzusetzen. Ebenso sollten Sie neben einer Virenschutzlösung auch eine geeignete Client-Firewall nutzen. Speziell, wenn es sich bei den Systemen um mobile Geräte wie Notebooks handelt, sollten Sie auf eine Firewall nicht verzichten. Blockieren Sie entsprechend den eingehenden und ausgehenden Verkehr, sodass nur die nötigsten Kommunikationsbeziehungen gestattet sind.

Aktueller Virenschutz

Installieren Sie einen zuverlässigen Virenschutz und konfigurieren Sie diesen entsprechend Ihren Bedürfnissen. Eine wichtige Rolle dabei spielen der Echtzeitschutz und regelmäßige Scans. Sorgen Sie außerdem dafür, dass die Virensignaturen mindestens einmal täglich aktualisiert werden. Nur ein aktueller Virenschutz ist in der Lage, einen ausreichenden Schutz zu gewährleisten. Generell empfiehlt sich der Einsatz einer unternehmenstauglichen Virenschutzlösung. Diese sollte eine eigene Managementkonsole besitzen und sich an Ihre Infrastruktur anpassen lassen können.

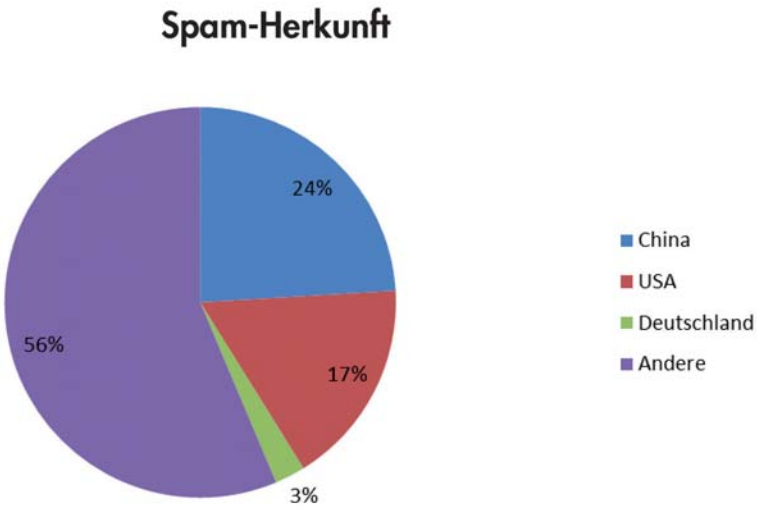

Bild 2: China und die USA sind die größten Spamschleudern

Mithilfe der Managementkonsole sollte es möglich sein, Agenten an die entsprechenden Systeme zu verteilen. Die Managementkonsole sollte Sie zudem über potenzielle Gefährdungen informieren und dementsprechend über eine Alarmierung, vorzugsweise per E-Mail, verfügen. Nur so können Sie zeitnah auf Gefährdungen reagieren und geeignete Maßnahmen etwa durch das Trennen eines Rechners vom Netzwerk und der anschließenden Bereinigung durchführen. Neben einem grundlegenden clientbasierten Virenschutz, den Sie regelmäßig aktualisieren und mit den neusten Signaturen ausstatten, sollten Sie zudem auf eine Engine in der Firewall und auf eine dedizierte Anti-Spam-Lösung zurückgreifen.

Sicher surfen

Neben den üblichen Sicherheitsmaßnahmen zum Schutz vor Malware sollten Sie zusätzlich zu einer geeigneten System-Härtung zwingend auch eine entsprechende Browser-Härtung durchführen. Prüfen Sie auch, ob der Einsatz eines zweiten, alternativen Browsers für Ihre Mitarbeiter einen Mehrwert bietet. Bedenken Sie dabei allerdings das notwenige Patch-Management. So könnten Anwender nach Bekanntwerden einer Sicherheitslücke einen alternativ Browser nutzen. Erst nach Behebung der Sicherheitslücke würden Sie dann die Nutzung des ersten Browsers wieder freigeben.

Auch den Einsatz von sogenannten Browser Add-ons sollten Sie prüfen. So sind kostenlos beispielsweise Erweiterungen verfügbar, die die Sicherheit erheblich erhöhen können. Hierzu zählen unter anderem Add-ons wie Adblock Plus, NoScript oder QuickJava. Adblock Plus verhindert nicht gewollte Werbeeinblendungen (die nur zu oft mit Schadcode versehen sind) und QuickJava erlaubt es, Anwendungen wie Java, JavaScript Flash und ähnliches per Mausklick im Browser zu aktivieren und zu deaktivieren. Das ist auch interessant für sicherheitsrelevante Abteilungen, die dennoch Zugang zum Internet benötigen. Hierfür bieten sich besonders abgespeckte Browser mit minimaler Angriffsfläche an.

Mitarbeiter sensibilisieren

Zum Schluss müssen Sie natürlich die Mitarbeiter in Hinblick auf Sicherheitsgefahren sensibilisieren. Hierfür bieten sich regelmäßige Inhouse-Schulungen sowie kompakte und leicht verständliche Handouts oder Intranet-Seiten mit den wichtigsten Verhaltensregeln an. Das Spektrum der Mitarbeiter reicht dabei vom Geschäftsführer bis hin zum Reinigungspersonal. Seien Sie sich bewusst, dass oft das schwächste Glied in der Kette zum Opfer wird. Vermitteln Sie Ihren Mitarbeitern ein gesundes Misstrauen und informieren Sie die Anwender regelmäßig über neue Angriffsmethoden. Versuchen Sie darüber hinaus, dem reisenden Personal Grundsätze von vertraulichen Gesprächen zu vermitteln. Vertrauensvolle Telefonate an Bahnhöfen oder an Flughäfen sollten vermieden oder zumindest abseits geführt werden. Ebenso sollten Arbeiten am Notebook oder Smartphone nicht ohne eine Sichtschutzfolie durchgeführt werden, um ein Mitlesen von Informationen zu verhindern. *(dr)*