Landesbeauftragte
für Datenschutz
und Akteneinsicht

Sichern Sie Ihr Smartphone!

Ergebnisse einer Umfrage auf dem Tag der offenen Tür im Landtag Brandenburg am 6. April 2019

Die Sicherheit von Smartphones war Thema eines Informationsstandes der Landesbeauftragten auf dem Tag der offenen Tür im Landtag Brandenburg am 6. April 2019. Zunächst hat uns interessiert, wie die einzelnen Teilnehmerinnen und Teilnehmer sich selbst einschätzen: Sichern sie ihr Smartphone sehr gut, gut oder nicht so gut? Jeder, der dies wollte, konnte es uns in spielerischer Weise mitteilen. Anschließend wollten wir noch wissen, welche Sicherheitsmaßnahmen die Besucherinnen und Besucher denn konkret umsetzen. Eine – selbstverständlich anonyme – Umfrage sollte darüber Aufschluss geben. Die unerwartet rege Beteiligung haben wir zum Anlass genommen, die Ergebnisse auszuwerten – auch wenn die 215 Antworten sicher nicht repräsentativ sind:

Frage 1: Nutzen Sie Zugangssperren bei Ihrem Smartphone?

Um bei Verlust oder Diebstahl des Mobiltelefons einen Basisschutz vor unbefugtem Zugriff auf persönliche Daten zu gewährleisten, **nutzten 83% der Befragten** eine Zugangssperre bei ihrem Smartphone.

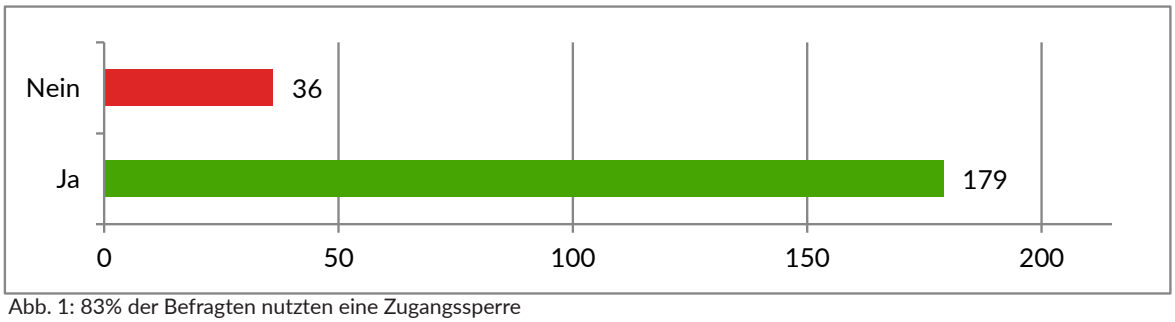

Abb. 1: 83% der Befragten nutzten eine Zugangssperre

Grundsätzlich sollten für jedes Smartphone Zugangssperren wie z. B. Displaysperren beispielsweise durch Zahlencodes, Wischmuster, Fingerabdruck oder Gesichtserkennung aktiviert sein. Die unbefugte Nutzung der SIM-Karte lässt sich durch eine PIN-Abfrage verhindern. Sensible Anwendungen, wie Online-Banking sind zusätzlich mit einer PIN oder einem Passwort zu schützen. Wichtige und sensible Daten, die auf dem Mobiltelefon gespeichert sind, sollten gegen einen unbefugten Zugriff verschlüsselt werden. Eine weitere Maßnahme bei einem Gerätediebstahl oder -verlust wäre, die persönlichen Daten auf dem Smartphone aus der Ferne mit einer vertrauenswürdigen App zu löschen. Die SIM-Karte sollte zeitnah beim Vertragspartner gesperrt werden, damit niemand mehr Kosten verursacht.

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht
Stahnsdorfer Damm 77 · 14532 Kleinmachnow · E-Mail: Poststelle@LDA.Brandenburg.de · www.LDA.Brandenburg.de
Fingerprint: E899 5780 7F65 F282 8CAC C504 37F3 83FE 0844 834D

Frage 2: Installieren Sie regelmäßig Sicherheitsupdates?

Auch in Bezug auf die zweite Frage „Installieren Sie regelmäßig aktuelle Sicherheitsupdates?“ lassen sich positive Schlüsse ziehen, denn **74% der Befragten** gaben an, dies zu tun.

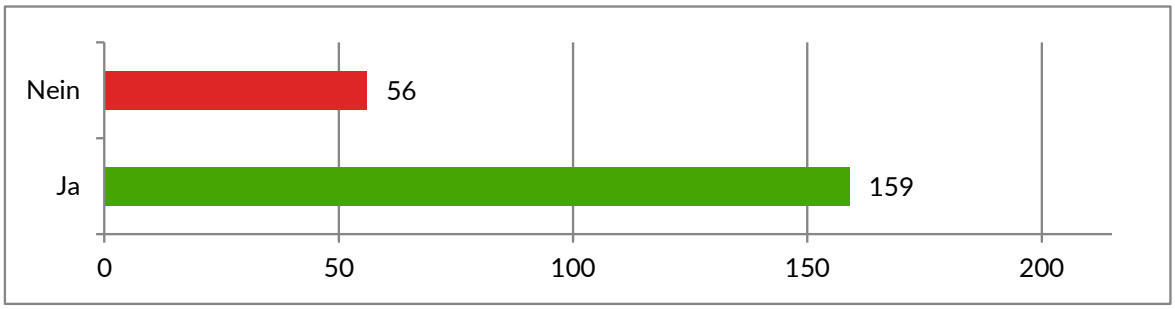

Abb. 2: 74% der Befragten updaten regelmäßig die Software ihrer Smartphones

Sobald Updates von Apps und dem Betriebssystem zur Verfügung stehen, sollten diese umgehend installiert werden. Schwachstellen und Sicherheitslücken können so schnell geschlossen werden. Angreifer könnten diese sonst ausnutzen und die Kontrolle über das Smartphone übernehmen oder Schadsoftware auf das Mobiltelefon aufspielen. Vorzugsweise sollte die Installation der Sicherheitsupdates über die Funktion „Automatische Updates“ erfolgen. Vorsicht ist jedoch vor „gefälschten“ Updates geboten, die von Betrügern in Umlauf gebracht werden. Die neue Software-Version sollte nur installiert werden, wenn die Update-Empfehlung in der vertrauten Form erscheint und das Update von einem vertrauenswürdigen Anbieter stammt. Nach der Installation wird empfohlen, zu kontrollieren, welche neuen Berechtigungen mit dem Update verbunden sind. Gegebenenfalls sind diese zu ändern.

Frage 3: Erstellen Sie regelmäßig Daten-Backups auf externen Speichermedien?

Regelmäßige Daten-Backups setzten allerdings nur **42% der Befragten** um. Eine mögliche Erklärung für die geringere Nutzungsrate, im Verhältnis zu den oben bereits besprochenen Methoden, könnte die komplexere technische Umsetzung sein.

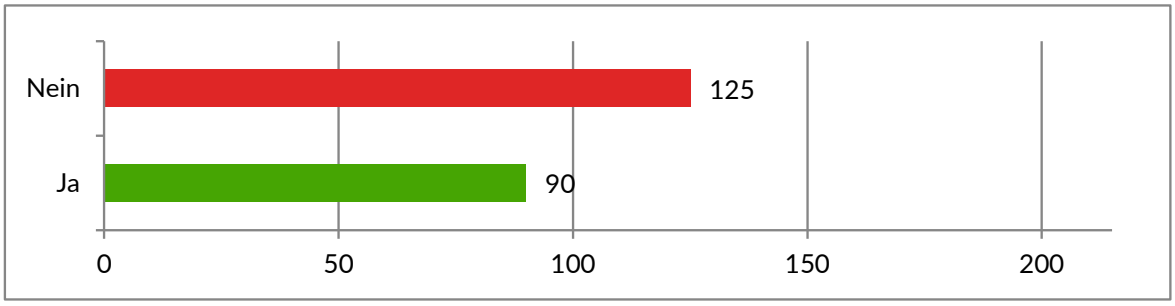

Abb. 3: Nur 42% der Befragten führen regelmäßig Daten-Backups durch

Wird regelmäßig ein Daten-Backup auf externen Speichermedien erstellt, kann sich jedoch die Nutzerin oder der Nutzer im Falle eines Diebstahles, bei einer digitalen Erpressung oder bei technischen Problemen grundsätzlich sicher sein, dass die Daten nicht verloren gehen und jederzeit wiederherstellbar sind.
Am sichersten ist es, ein Backup auf einem externen Computer oder einer externen Festplatte durchzuführen. Allerdings bedarf es oft, je nach Umfang der zu sichernden Daten, eines gewissen Aufwandes. Eine Möglichkeit, die zwar weniger Aufwand bedeutet, aber aus Datenschutzgründen problematisch sein kann, ist die Speicherung der Daten in der Cloud. In diesem Fall wird dringend empfohlen, darauf zu achten, dass der Cloud-Anbieter hinreichende Sicherheitsmaßnahmen umsetzt (z. B. verschlüsselte Übertragung, Schutz vor Auslesen der Daten durch Dritte).

Frage 4: Haben Sie Ortungsdienste wie GPS deaktiviert wenn Sie diese nicht benötigen?

Eine Vielzahl der Teilnehmerinnen und Teilnehmer war sich der Risiken bewusst, die eine permanente und uneingeschränkte Nutzung von Ortungsdiensten wie GPS bedeuten kann. **59% der Befragten** achteten auf einen bewussten Umgang mit diesem Dienst und deaktivierten ihn, wenn sie ihn nicht benötigten.

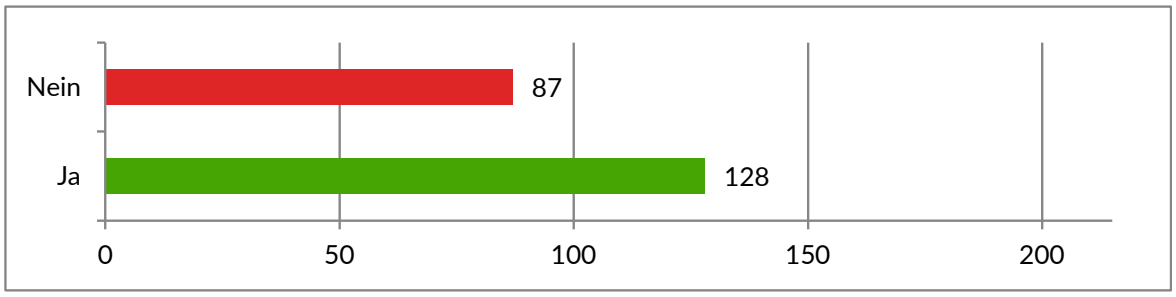

Abb. 4: 59% der Befragten beenden Ortungsdienste nach der Nutzung

Durch GPS erhobene Positionsdaten könnten sonst leicht an Dritte weitergegeben oder für die Aufzeichnung von Bewegungsprofilen verwendet werden. Dies gilt insbesondere für Fotos, die mit dem Mobiltelefon aufgenommen und im Internet veröffentlicht werden, soweit sie GPS-Daten enthalten.

Frage 5: Ist Ihr WLAN deaktiviert, wenn Sie dieses nicht benötigen?

Etwas mehr als **50% der Befragten** achteten nicht auf die Deaktivierung der WLAN-Schnittstelle ihres Mobilgerätes, wenn sie diese nicht benötigten.

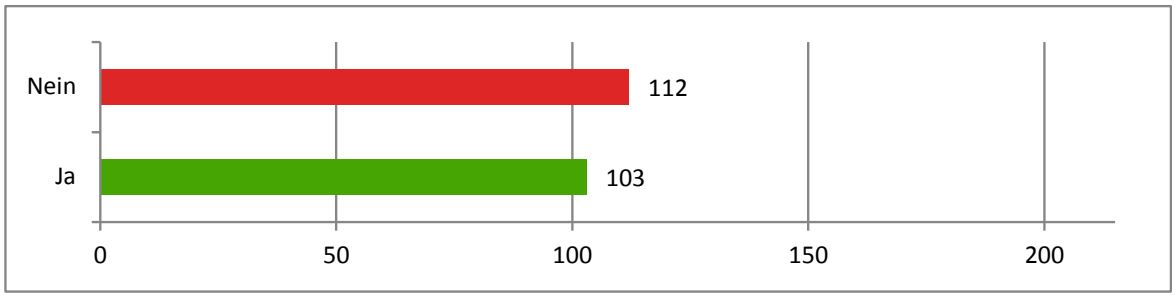

Abb. 5: Mehr als 50% der Befragten deaktivieren nicht ihr WLAN nach der Nutzung

Freigeschaltete drahtlose Schnittstellen wie WLAN, Bluetooth oder NFC (Near Field Communication) sind für Kriminelle eine gute Möglichkeit, Schadsoftware auf das Smartphone zu spielen. Möglicherweise war dies der anderen Hälfte der Befragten nicht bewusst. Doch sollte beachtet werden, dass durch infizierte Smartphones z. B. ohne Wissen der Nutzerin oder des Nutzers kostenpflichtige Telefonnummern angewählt oder Kurzmitteilungen mit Links zu schadhaften Webseiten an Personen aus dem internen Adressbuch gesendet werden könnten.

Fazit

Insgesamt lässt sich das Bewusstsein der Befragten für die Sicherheit von Smartphones durchaus positiv bewerten. Bei den Fragen zu Zugangssperren und Sicherheitsupdates ist festzuhalten, dass die große Mehrheit der Befragten Mindeststandards des Datenschutzes für Mobilgeräte nutzt. Die Antworten auf die anderen Fragen lassen durchaus den Schluss zu, dass ein großer Anteil der Befragten sich mit diesen Problematiken auseinandersetzt.