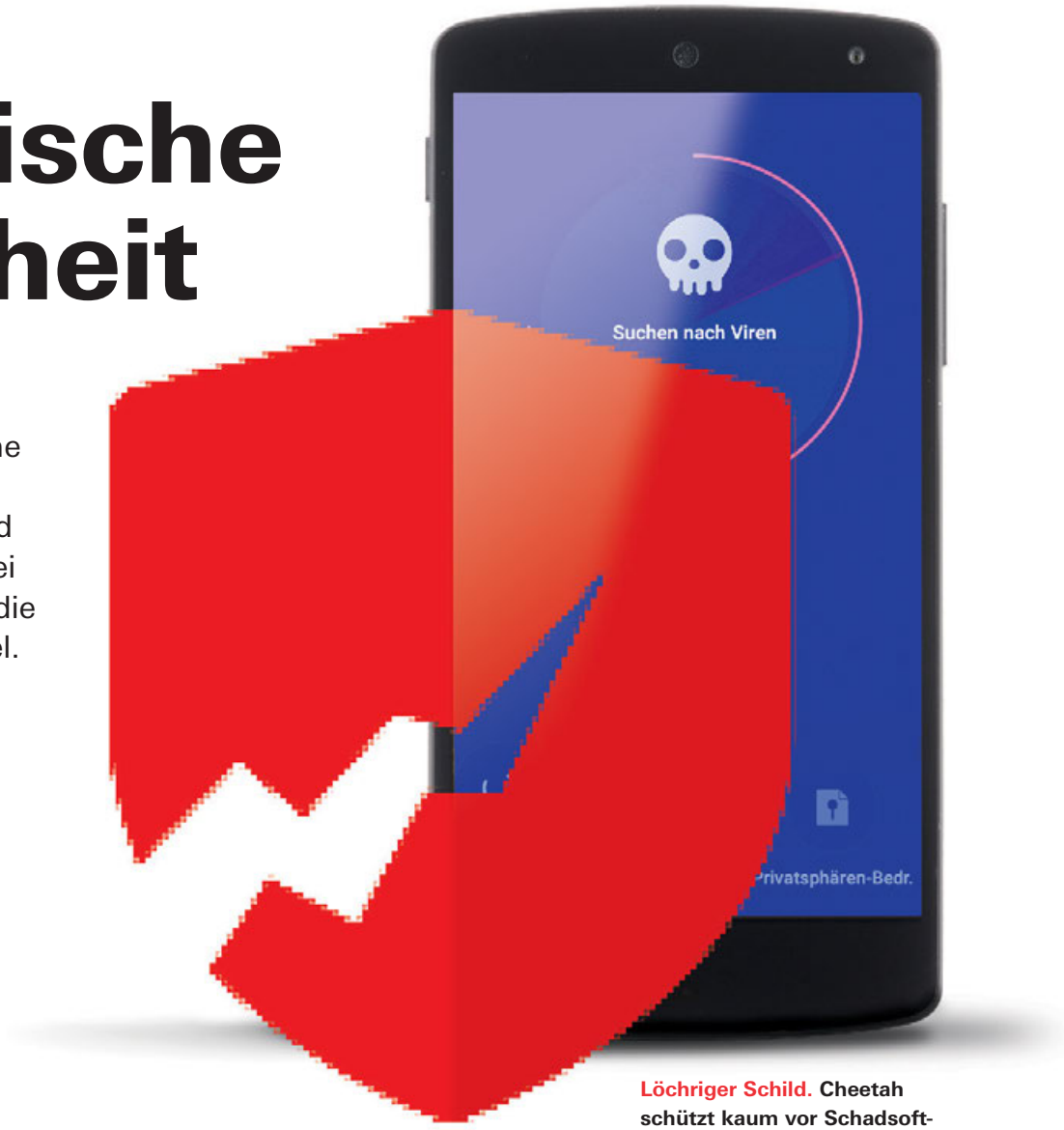
Trügerische Sicherheit

Sicherheits-Apps Längst nicht alle Schutzprogramme für Android-Smartphones wehren Schadsoftware und Betrüger zuverlässig ab. Bei Verlust des Handys reicht die Hilfe der Google-Bordmittel.



Löchriger Schild. Cheetah schützt kaum vor Schadsoftware und Betrüger-Websites.

Einkaufen im Internet, Onlinebanking, E-Mails: All das findet heute nicht mehr nur am PC, sondern auch auf dem Handy statt. Viele wollen darum auch ihr Smartphone mit Sicherheitssoftware schützen, wie das beim PC selbstverständlich ist. Für Android-Handys ist ein breites Angebot an Sicherheits-Apps verfügbar. Doch unser Test zeigt: Längst nicht alle schützen zuverlässig.

Wir prüften 17 Apps für Android-Handys und verglichen sie mit dem Schutzschild, der auf Geräten mit dem Google-Betriebssystem vorinstalliert ist. Das Ergebnis ist zwiespältig. Insgesamt sind 9 Apps gut, eine davon mit sehr gutem Schutz vor Schadsoftware und betrügerischen Webseiten: die kostenpflichtige Version von Eset. Von AVG ist eine Gratis-App vertreten, die gut vor beidem schützt. Sie alle bieten deutlich mehr Schutz als der vorinstallierte Google-Schild, der sich als mangelhaft erwies. Etliche Apps jedoch versagen, besonders beim Schutz vor betrügerischen Webseiten. Ist das Handy verloren oder geklaut, helfen nur wenige Apps besser als die vorinstallierte Google-Hilfe (siehe Tabelle S. 46/47). Die wichtigsten Antworten zum Test:

Braucht ein Handy Sicherheitssoftware?

Weniger zwingend als ein PC. Mobile Betriebssysteme wie Android und iOS (siehe Kasten S. 46) sind aufgrund ihrer Sys- ▶

Unser Rat

Beste Sicherheits-App im Test ist **Eset Mobile Security & Antivirus**. Für 10 Euro im Jahr schützt das Programm sehr gut vor Schadsoftware und vor betrügerischen Webseiten („Phishing“). Beste kostenlose App ist die **Gratisversion von AVG Antivirus** mit rundum guter Schutzfunktion. Gute Hilfe bei Verlust leistet Google für Android-Handys auch schon ohne zusätzliche Sicherheits-Apps.

temarchitektur nicht so anfällig für Hacker-Angriffe wie PC-Systeme. Ist eine zusätzliche Schutzsoftware gut gemacht, kann sie die Sicherheit aber erhöhen. Wie sinnvoll das ist, hängt vor allem vom Nutzerverhalten ab. Wer sich gewissenhaft an die wichtigsten Sicherheitsregeln hält (siehe Kasten S. 45), braucht keine Schutz-App.

Was sollten Sicherheits-Apps leisten?

Traditionell dient Sicherheitssoftware zum Schutz vor Schadprogrammen, die zum Beispiel das Handy sperren, um Schutzgeld zu erpressen. Wir erwarten zudem, dass die Apps ihre Nutzer vor gefälschten Websites warnen. Mit solchen „Phishing-Seiten" (von englisch „Password Fishing", angeln nach Passwörtern) wollen Betrüger Zugangsdaten zu wichtigen Online-Diensten abgreifen. Außerdem sollten die Apps verlorene oder geklaute Handys aus der Ferne orten und sperren können.

Wie kommt Schadsoftware aufs Handy?

Anders als beim PC gibt es für Handy-Systeme praktisch keine „Viren", die sich von selbst verbreiten. Daher müssen Bösewichte Smartphone-Nutzer dazu bringen, die Schadprogramme eigenhändig zu installieren – etwa indem sie sie als nützliche Systemerweiterung oder als begehrte Raubkopie tarnen. Wer dem Download widersteht und Apps nur direkt aus Googles App-Store lädt, ist auch ohne Sicherheitssoftware gegen derlei Gefahren gut gefeit.

Wie gut schützen die Apps vor Schädlingen?

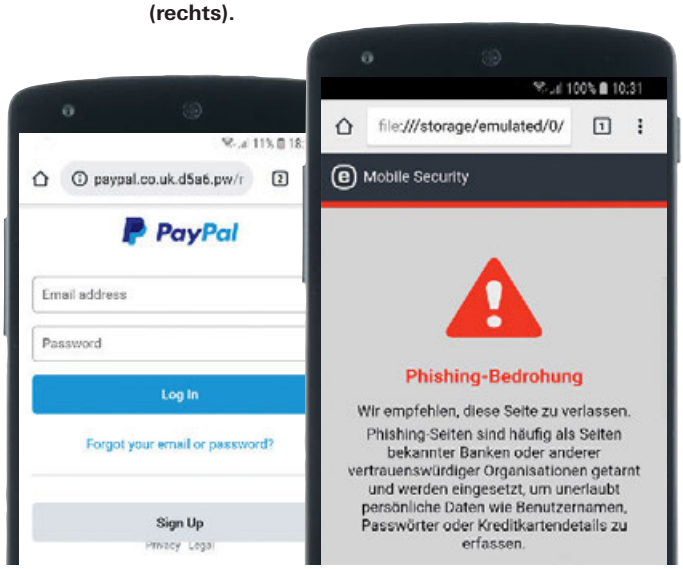
Sicherheits-Apps sollen Schadsoftware im Handyspeicher finden und jeden Versuch verhindern, sie zu installieren. Wir haben das mit 2000 Schadprogrammen geprüft. Erfreulich: Etliche Apps erkannten sie fast alle. Der auf Android-Handys vorinstallierte Schutzschild „Google Play Protect" fand dagegen nur etwas mehr als die Hälfte. Am schlechtesten schützt Cheetah: Es fand nur knapp 170 der 2000 Schädlinge. Nervig ist die App von Sophos: Sie erkennt zwar die meisten Schädlinge, schlägt aber auch bei vielen harmlosen Dateien Alarm.

Wie gut schützen die Apps vor Phishing?

Wenn der Nutzer versucht, eine gefälschte Website aufzurufen, sollte eine Sicherheits-App Alarm schlagen. Manche analysieren hierfür den Datenverkehr des verwendeten Internetbrowsers. Andere stellen einen eigenen Browser mit integriertem Phishing-Schutz bereit, mit dem Nutzer ins Internet gehen müssen, um sicher zu surfen. Am besten schützt die kostenpflichtige App von Eset: Sie warnte im Test vor 227 von 250 Phishing-Seiten. Viele andere schützen dagegen kaum oder gar nicht vor Phishing – auch Googles eigene Schutzfunktion „Safe Browsing" nicht. Im Test vor drei Jahren lieferte sie noch sehr gute Ergebnisse.

Was hilft, wenn das Handy weg ist?

Beim Verlust des Handys stellt sich die Frage: Ist es gestohlen – oder nur zu Hause liegen geblieben? Hier hilft der vorinstallierte Ortungsdienst von Google: Alle Android-Handys, die mit einem Google-Konto verknüpft sind, lassen sich vom jeweiligen Kontoinhaber über die Google-Website aus der Ferne orten (siehe Foto S. 45). Stellt sich dabei heraus, dass das Gerät in den Händen von Dieben ist, kann man es aus der Ferne sperren oder alle Daten löschen. Das ist bei Android-Handys (wie auch bei iPhones, siehe S. 46) ab Werk so gut gelöst, dass eine Zusatz-App kaum nötig ist. Besser als Google selbst helfen bei Verlust des Handys nur Norton und die Bezahlversionen von AVG



Guter Schutz. Mit gefälschten Websites greifen Hacker Passwörter ab (links: gefälschte Paypal-Seite). Die kostenpflichtige Version der Eset-App erkennt die meisten dieser Phishing-Versuche (rechts).

Schlechter Schutz. BullGuard sperrt Handys per SMS – das Passwort zum Entsperren erscheint aber auf vielen Handys im Sperrschirm.

FOTOS: STIFTUNG WARENTEST; ISTOCKPHOTO

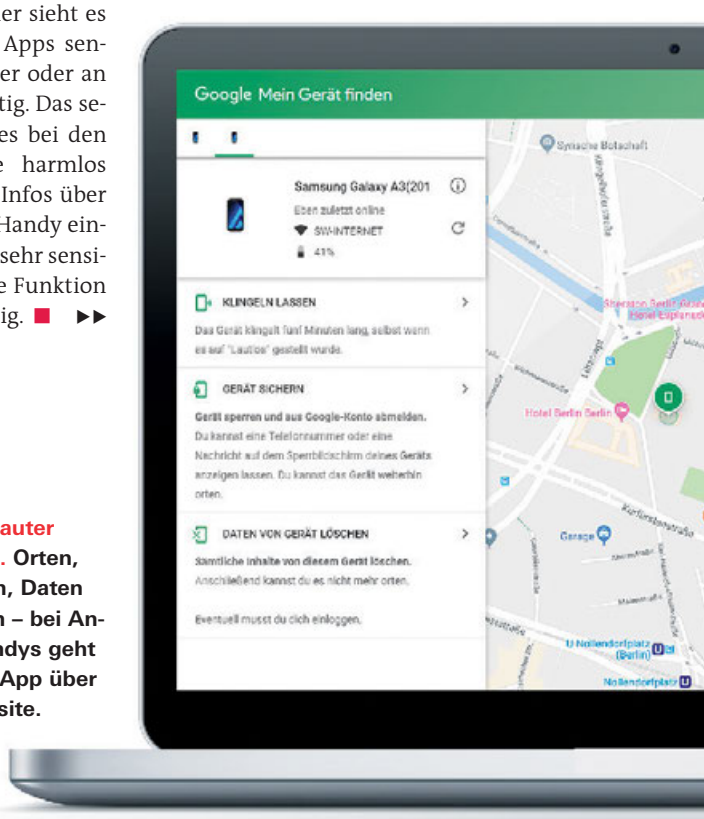
und Eset. Das Orten aus der Ferne klappt allerdings nur, solange das Handy eine Internetverbindung hat und seine Ortungsfunktion eingeschaltet ist.

Wie funktioniert die Fernortung per SMS?

Einige Apps können ein verlorenes Handy nicht nur per Internet orten und sperren, sondern auch per SMS. Manche gehen ausschließlich diesen Weg. Das ist nützlich, wenn das Handy keine Internetverbindung hat. Nutzer senden einen SMS-Befehl ans verlorene Handy. Doch mehrere Apps öffnen dabei neue Sicherheitslücken. Nutzer von BullGuard und Dr. Web müssen in der Sperr-SMS ans vermisste Handy ein Passwort zum Entsperren festlegen. Das Problem: Android-Handys sind meist so voreingestellt, dass sie Inhalte eingehender SMS auf dem Sperrbildschirm anzeigen – und damit dem Dieb das Passwort zum Entsperren. Bei Avast lässt sich der Sperrbildschirm leicht umgehen.

Belasten die Apps Akku und Prozessorleistung?

Die technische Belastung der Handys hält sich in Grenzen. Die Apps beanspruchen weder den Akku noch die Prozessorleistung oder das Datenvolumen besonders stark. Niemand muss auf Sicherheits-Apps verzichten, weil sie sein Handy zu langsam machen würden. Problematischer sieht es beim Datenschutz aus: Etliche Apps senden mehr Daten an den Anbieter oder an Marketing-Unternehmen als nötig. Das sehen wir kritisch – auch wenn es bei den meisten Apps vergleichsweise harmlos ausfällt. So senden die meisten Infos über den Netzbetreiber, bei dem das Handy eingebucht ist. Das sind zwar keine sehr sensiblen Informationen, aber für die Funktion der Apps sind sie nicht notwendig. ■ ▶▶



Eingebauter Schutz. Orten, sperren, Daten löschen – bei Android-Handys geht das auch ohne App über die Google-Website.

Android-Handys sicher nutzen

Wer die Bedrohungen kennt und die wichtigsten Schutzregeln befolgt, braucht fürs Android-Handy nicht zwingend eine Sicherheits-Software. Auch wer auf zusätzlichen Schutz per App baut, sollte diese Regeln beherzigen, denn hundertprozentigen Schutz kann keine App leisten.

Bedrohung: Schadsoftware. Schadprogramme für Android verbreiten, sich nicht von selbst. Stattdessen bringen Hacker Handy-Nutzer mit Tricks dazu, verseuchte Apps selbst zu installieren.
Schutz: Apps nur von Google. Installieren Sie Apps nur direkt aus dem Google Play Store – und nur solche, die dort schon einige Wochen verfügbar sind. Lassen Sie in den Sicherheitseinstellungen des Handys die Option, „Apps aus unbekannten Quellen" zu installieren, ausgeschaltet.

Bedrohung: Mobilfunk-Abzocke. Über Schadsoftware oder durch Anklicken von Werbebannern – Abzocker schröpfen ihre Opfer auch mit Abo-Fallen und SMS-Diensten, die über die Mobilfunkrechnung abgerechnet werden.
Schutz: Drittanbietersperre. Lassen Sie für Ihren Handyanschluss eine Drittanbietersperre einrichten. Dies geht zum Beispiel über die Telefon-Hotline Ihres Mobilfunkanbieters.

Bedrohung: Phishing. Über gefälschte Webseiten, die aussehen wie die von großen Onlinehändlern, Mail- oder Bezahldiensten, gelangen Hacker an Zugangsdaten argloser Nutzer. Meist geraten die Opfer über Links in gefälschten E-Mails auf solche Betrüger-Seiten.
Schutz: Nie über Links anmelden. Misstrauen Sie E-Mails – sie können gefälscht sein. Loggen Sie sich bei Onlinediensten nie über einen Link aus einer E-Mail ein. Tippen Sie stattdessen im Internetbrowser von Hand die Web-Adresse des jeweiligen Anbieters ein und melden sich dann dort an.

Bedrohung: Diebstahl. Zusätzlicher Schaden kann entstehen, wenn ein Dieb Ihr Handy entsperren und so auf Ihre Kosten telefonieren oder Zugang zu Ihrem E-Mail-Konto erlangen kann.
Schutz: Sperre und Fernortung. Sichern Sie Ihr Handy mit einer persönlichen Identifikationsnummer (Pin). Ist Ihr Handy weg, können Sie es über die Google-Website aus der Ferne orten und sperren. Melden Sie sich dafür mit Ihrem Google-Konto unter google.de an und nutzen Sie dort die Funktion „Smartphone suchen" (siehe Foto oben). Fürs Orten muss am Handy die Ortungsfunktion aktiv sein.

Sicherheits-Apps für Android: Längst nicht alle schützen gut

Produkt		Eset Mobile Security & Antivirus	Kaspersky Antivirus und Handy Schutz	AVG Antivirus	Avira Antivirus Security	Bitdefender Mobile Security & Antivirus	Norton Antivirus & Sicherheit	AVG AntiVirus (Gratisversion)	Lookout Antivirus & Sicherheit
Preis für eine Jahreslizenz ca. (Euro)		**10,00**	**17,00**	**8,50**	**7,95**	**9,95**	**17,00**	**Kostenlos**	**25,00**
test - **QUALITÄTSURTEIL**	**100 %**	**GUT (1,6)**	**GUT (1,7)**	**GUT (1,9)**	**GUT (2,0)**	**GUT (2,0)**	**GUT (2,0)**	**GUT (2,1)**	**GUT (2,3)**
Schutzfunktion	**45 %**	**sehr gut** (1,5)	**sehr gut** (1,4)	**gut** (2,1)	**sehr gut** (1,2)	**gut** (1,9)	**gut** (2,5)	**gut** (2,1)	**gut** (2,4)
Schutz vor Schadsoftware		++	++	+	++	++	++	+	○
Schutz vor betrügerischen Webseiten („Phishing“)		++	+	+	+	○	⊖*)	+	+
Hilfe nach Verlust	**35 %**	**gut** (2,1)	**gut** (2,5)	**gut** (2,2)	**befried.** (3,1)	**befried.** (2,6)	**gut** (1,9)	**gut** (2,4)	**befried.** (2,8)
Orten		+	+	+	○	+	+	+	+
Sperren		++	+	++	○	⊖	+	+	○
Löschen		○	○	+	○	+	+	+	○
Handhabung	**15 %**	**sehr gut** (1,1)	**sehr gut** (0,9)	**sehr gut** (1,1)	**sehr gut** (1,4)	**sehr gut** (1,1)	**sehr gut** (1,0)	**sehr gut** (1,4)	**sehr gut** (1,3)
Installieren und Deinstallatieren		++	++	++	+	++	++	++	++
Benutzen		++	++	++	++	++	++	++	++
Smartphonebelastung	**5 %**	**gut** (1,6)	**gut** (1,6)	**gut** (1,7)	**gut** (1,7)	**sehr gut** (1,4)	**sehr gut** (1,4)	**gut** (1,8)	**gut** (1,8)
Datensendeverhalten[1)]	**0 %**	**unkritisch**	**kritisch**	**kritisch**	**kritisch**	**kritisch**	**kritisch**	**kritisch**	**unkritisch**
Ausstattung/Technische Merkmale									
Geprüfte Version		4.1.20.0	11.17.4.1024	6.10.13	5.3.0	3.3.025.570	4.2.1.4174	6.10.13	10.23.1-c52f43f
Online: Orten/Sperren/Löschen		■/■/■	■/■/■	■/■/■	■/■/■	■/■/■	■/■/■	■/■/■	■/■/■
Per SMS: Orten/Sperren/Löschen		■/■/■	❑/❑/❑	❑/❑/❑	❑/❑/❑	■/■/■	■/■/■	❑/❑/❑	❑/❑/❑
Löschen	Kontakte/Kalender/E-Mails	■/■/■	■/■/■	■/■/■	■/■/■	■/■/■	■/■/■	■/■/■	■/■/■
	Google-Konto/Gerät zurücksetzen	■/■	■/■	■/■	■/■	■/■	■/■	■/■	■/■
Bei Wechsel der Sim-Karte	Sperre/Warnung	■/■	■/■	■/■	❑/❑	❑/❑	■/❑	❑/❑	❑/■
	Info zur neuen Rufnummer	❑	❑	❑	❑	❑	❑	❑	❑

Bewertungsschlüssel der Prüfergebnisse:
++ = Sehr gut (0,5–1,5). + = Gut (1,6–2,5). ○ = Befriedigend (2,6–3,5).
⊖ = Ausreichend (3,6–4,5). — = Mangelhaft (4,6–5,5).

Datensendeverhalten: unkritisch, kritisch, sehr kritisch.
Bei gleichem Qualitätsurteil Reihenfolge nach Alphabet.
***) Führt zur Abwertung** (siehe „So haben wir getestet“ unten Seite 46/47).

■ = Ja.
❑ = Nein.

Keine Sicherheits-Apps fürs iPhone

Das Apple-System iOS, das auf iPhones und iPads läuft, ist geschlossener als Android und damit noch weniger angreifbar. Sicherheits-Apps sind darum fürs iPhone überflüssig.

Schutz vor Schadsoftware. Anders als bei Android-Handys lassen sich Apps für iOS-Geräte ausschließlich aus Apples App Store laden. Apple prüft die dort eingereichten Programme auf Schadfunktionen. So ist die Infektion von iPhones mit bösartiger Software praktisch ausgeschlossen.

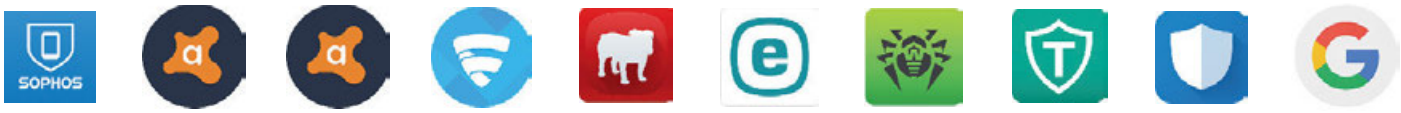
Schutz vor Phishing. Apples Browser „Safari“ warnt vor betrügerischen Websites. Im Test war seine Erkennungsrate aber schlechter als die der besten Sicherheits-Apps. Wichtigster Schutz vor Phishing bleibt Vorsicht im Umgang mit Mails und Webseiten.

Hilfe bei Verlust. iPhones lassen sich wie Android-Geräte aus der Ferne orten und sperren. Fürs Sperren muss auf dem iPhone die Menü-Einstellung „Mein iPhone suchen“ aktiviert sein, fürs Orten auch die Ortungsfunktion.

So haben wir getestet

Im internationalen Gemeinschaftstest unter Federführung der Stiftung Warentest: 17 Sicherheits-Apps für Android-Geräte sowie die Sicherheitsfunktionen, die auf Android-Handys vorinstalliert sind. Wir luden die Apps im Juli 2018 aus dem Google Play Store herunter. Die Preise sind die von uns dabei bezahlten.

Untersuchungen: Alle Prüfungen erfolgten auf Smartphones des Typs Samsung Galaxy S9 unter dem Betriebssystem Android 8. Bei den Prüfungen zur Smartphonebelastung nutzten wir zusätzlich ein weniger leistungsstarkes Smartphone vom Typ Huawei Y7. Die Tests der Schutzfunktion liefen mit allen Apps nahezu zeitgleich.



Sophos Mobile Security	**Avast** Mobile Antivirus & Virenschutz	**Avast** Mobile Antivirus & Virenschutz (Gratisversion)	**F-Secure** Safe Internet Security & Mobile Antivirus	**BullGuard** Mobile Security and Antivirus (Gratisversion)	**Eset** Mobile Security & Antivirus (Gratisversion)	**Dr. Web** Security Space	**TrustGo** Antivirus & Mobile Security	**Cheetah Mobile** Security Master	**Google** Android vorinstallierte Sicherheitsfunktionen[2]
Kostenlos	**8,50**	**Kostenlos**	**15,00**	**Kostenlos**	**Kostenlos**	**7,00**	**Kostenlos**	**11,00**	**Kostenlos**
GUT (2,5)	**BEFRIEDIGEND (2,6)**	**BEFRIEDIGEND (2,6)**	**BEFRIEDIGEND (3,1)**	**BEFRIEDIGEND (3,3)**	**AUSREICHEND (4,2)**	**AUSREICHEND (4,4)**	**AUSREICHEND (4,5)**	**MANGELHAFT (5,0)**	**AUSREICHEND (4,1)**
gut (2,5)	**gut** (2,1)	**gut** (2,1)	**ausreich.** (4,0)	**ausreich.** (4,1)	**ausreich.** (4,2)	**mangelh.** (5,2)*)	**mangelh.** (5,5)*)	**mangelh.** (5,5)*)	**mangelh.** (5,5)*)
○	+	+	++	++	++	○	⊖	–	⊖
+	+	+	–*)	–*)	–*)	–*)	–*)	–*)	–*)
befried. (3,1)	**ausreich.** (3,7)*)	**ausreich.** (3,7)*)	**befried.** (2,9)	**befried.** (3,4)	**ausreich.** (4,3)*)	**ausreich.** (4,0)	**ausreich.** (3,7)	**mangelh.** (4,7)	**gut** (2,4)
⊖	+	+	○	+	⊖	⊖	⊖	○	+
○	–*)	–*)	○	–*)	⊖	–*)	+	–*)	+
○	○	○	○	○	–	○	–	–	+
sehr gut (0,9)	**sehr gut** (1,1)	**sehr gut** (1,4)	**sehr gut** (1,0)	**sehr gut** (1,4)	**sehr gut** (1,2)	**sehr gut** (1,3)	**sehr gut** (1,2)	**gut** (2,2)	**sehr gut** (1,2)
++	++	++	+	++	++	++	++	++	++
++	++	++	++	++	++	++	++	+	++
gut (1,7)	**gut** (1,6)	**gut** (1,7)	**gut** (2,2)	**sehr gut** (1,3)	**sehr gut** (1,5)	**sehr gut** (1,5)	**sehr gut** (1,3)	**sehr gut** (1,5)	**sehr gut** (1,2)
unkritisch	**kritisch**	**kritisch**	**kritisch**	**unkritisch**	**unkritisch**	**unkritisch**	**kritisch**	**kritisch**	Nicht bewertbar[3]
8.5.2765	6.11.4	6.11.4	17.4.0014003	14.0.9.172	4.1.20.0	12.3.0	3.1.0	4.6.4	Entfällt
❑/❑/❑	■/■/■	■/■/■	■/■/■	■/❑/■	❑/❑/❑	❑/❑/❑	■/■/■	■/■/■	■/■/■
■/■/■	❑/❑/❑	❑/❑/❑	❑/❑/❑	■/■/❑	■/■/❑	■/■/■	❑/❑/❑	❑/❑/❑	❑/❑/❑
■/■/■	■/■/■	■/■/■	■/■/■	■/■/■	❑/❑/❑	■/■/■	■/❑/❑	❑/❑/❑	■/■/■
■/■	■/■	■/■	■/■	■/■	❑/❑	■/■	❑/❑	❑/❑	■/■
❑/■	■/■	❑/❑	❑/■	❑/❑	❑/❑	■/■	■/❑	❑/■	❑/❑
■	❑	❑	❑	❑	❑	❑	❑	❑	❑

1) Urteil bezieht sich auf die im Datenstrom identifizierten Daten.
2) Auf Android-Handys vorinstallierte Funktionen, darunter Google Play Protect, der Safe-Browsing-Modus des Chrome-Browsers und die Funktion „Smartphone suchen".
3) Nicht bewertbar, da sich einzelne Daten nicht den geprüften Google-Sicherheitsfunktionen zuordnen lassen.

Schutzfunktion: 45 %

Den **Schutz vor Schadsoftware** prüften wir durch Download und Installation von 2 000 Schadprogrammen sowie durch Scan des Handyspeichers, in dem sich 2 000 Schadprogramme befanden. Die Häufigkeit von Fehlalarmen maßen wir anhand von mehr als 2 000 unschädlichen Apps. Den **Schutz vor betrügerischen Webseiten („Phishing")** prüften wir durch Aufrufe 250 betrügerischer Webseiten.

Hilfe nach Verlust: 35 %

Aus der Ferne **orteten**, **sperrten** und **löschten** wir die Smartphones je nach Verfügbarkeit der Anbieter-Webseite per App und per SMS. Die Durchführung und die angebotenen Funktionen (etwa Orten auch mit ausgeschalteter Ortungsfunktion, Alarme und Warnmeldungen, Löschen von Mail-Konten und des Speichers) wurden bewertet.

Handhabung: 15 %

Fünf Experten prüften das **Installieren und Deinstallieren** der Apps und das **Benutzen** (unter anderem von Menü, Navigation der App, Aussagekraft von Warnmeldungen).

Smartphonebelastung: 5 %

Wir bewerteten die Mehrbelastung des Akkus beim Betrieb der Sicherheits-Apps und beim Scannen sowie die Zeitdauer eines Scans. Auch bewerteten wir das verbrauchte Datenvolumen bei einem Scan und einer 24-stündigen Nutzung der App.

Datensendeverhalten: 0 %

Der Datenverkehr zwischen den Apps und Servern im Internet wurde aufgezeichnet und, falls erforderlich, entschlüsselt. Wir suchten unter anderem nach eindeutigen Gerätekennungen und Nutzerdaten, deren Übermittlung für das Funktionieren der App nicht notwendig ist.

Abwertungen

Abwertungen sorgen dafür, dass sich Produktmängel verstärkt auf das test-Qualitätsurteil auswirken. Folgende Abwertungen haben wir eingesetzt: Ab einer mangelhaften Schutzfunktion und einer ausreichenden Hilfe nach Verlust werteten wir das test-Qualitätsurteil ab. Ab einem ausreichenden Schutz vor betrügerischen Webseiten werteten wir das Urteil für die Schutzfunktion ab. Ab dem Urteil mangelhaft für das Sperren werteten wir das Urteil für die Hilfe nach Verlust ab. Sind die Urteile gleich oder nur geringfügig schlechter als diese Noten, ergeben sich nur geringe negative Auswirkungen. Je schlechter die Urteile, desto stärker ist der jeweilige Abwertungseffekt.