Educational Month
Cyber Security

Cyber-Angriffe abwehren – Schutz Ihrer mobilen Geräte

Presented by
Mario Bohum, Jasin Mehovic
und Franz Finke

16. November 2023

Herzlich willkommen! Ihre Online-Session startet gleich.

Schön, dass Sie dabei sind. Hören Sie uns einfach per Kopfhörer oder Lautsprecher zu.

Wir schalten die Mikrofone der Teilnehmer:innen stumm. Dann hören Sie alles besser. Auch alle Webcams sind automatisch deaktiviert.

Ihre Fragen können Sie über das Fragen-Fenster stellen. Der Moderator bringt Ihre Fragen entsprechend ein.

Agenda

00 Intro

01 Cyber-Angriffe auf mobile Endgeräte

02 Demo Hacker-Angriffe

03 Lookout und EMM

Heute für Sie in der Online-Session:

Mario Bohum

Senior Digital Presales Consultant
Vodafone

Jasin Mehovic

Director Channel Central Europe & EMEA SI´s
Lookout

Franz Finke

Sales Engineer DACH & EE
Lookout

Cyber-Angriffe auf mobile Endgeräte

01

Die Ära der Cyber Security

2019

Nutzen Sie O365?

2020

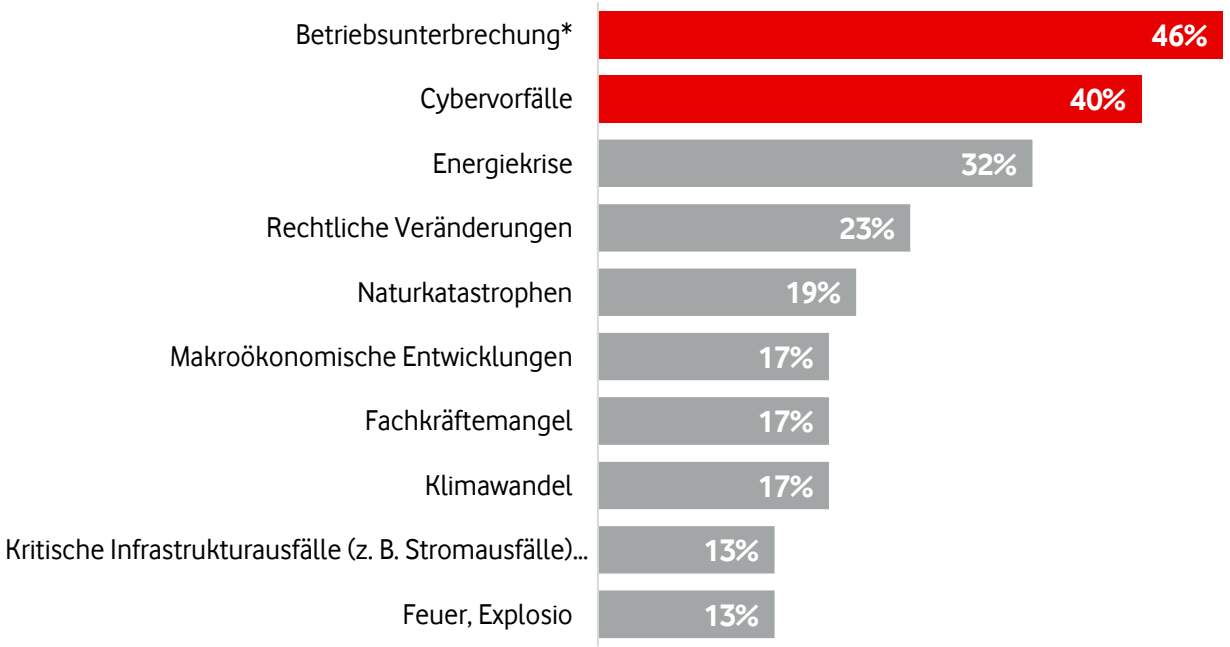
Homeoffice ...

2023

You've been hacked ...

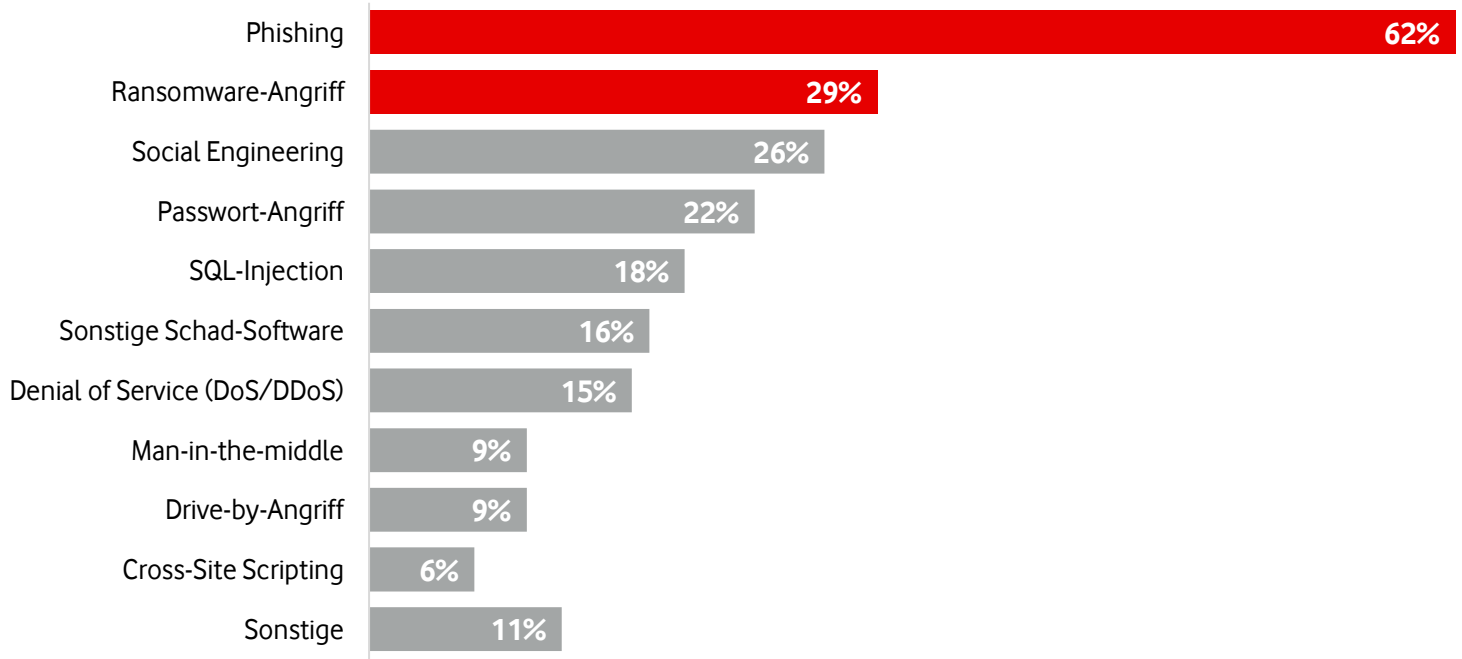
Cyber-Angriffe für zu den Top 2 Geschäftsrisiken weltweit

Top 10 Geschäftsrisiken in Deutschland in 2023



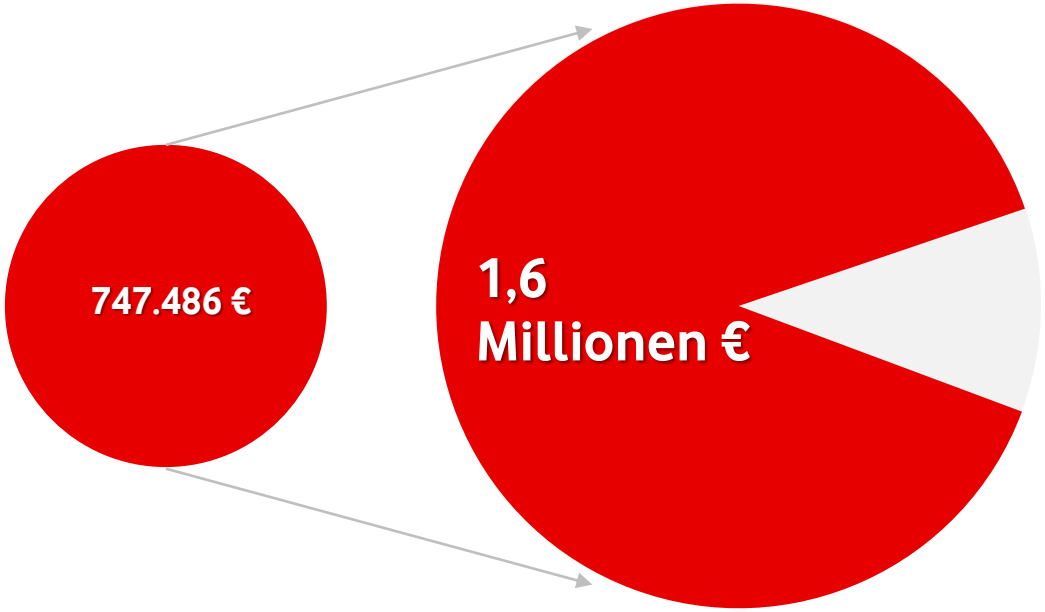
Quelle: Allianz Risk Barometer 2023
Die Zahlen stellen den Prozentsatz der Antworten aller Teilnehmer:innen dar, die geantwortet haben (925). Die Zahlen addieren sich nicht zu 100 %, da mehr als ein Risiko ausgewählt werden konnte.
* Meist durch Cybervorfälle ausgelöst.

Phishing und Ransomware bleiben die häufigsten Angriffsmethoden



Quelle: TÜV Cybersecurity Studie 2023

Cyber.Crime.Cash.
Lösegeld-Zahlung nur Bruchteil der Kosten



Quellen: Sophos - The State of Ransomware 2021; Coverware 2023

361.000 €

Durchschnittliche Lösegeld-Summe

- Die Kosten der Wiederherstellung des operativen Betriebs sind um den **Faktor 4,4 höher** als die Lösegeld-Summe
- Betriebsunterbrechung und Wiederherstellungskosten sind die Hauptkostentreiber nach einer Ransomware-Attacke
- **Downtime**: durchschnittlich **21 Tage**

Phishing – großes Problem auf kleinem Bildschirm

Phishing-Angriffe werden oft mit E-Mails in Verbindung gebracht. Jedoch können Phishing-Angriffe über eine Vielzahl von Messaging- und App-Plattformen erfolgen – vor allem auf Geräten, die sich in Privatbesitz befinden (BYOD).

Nr. 1

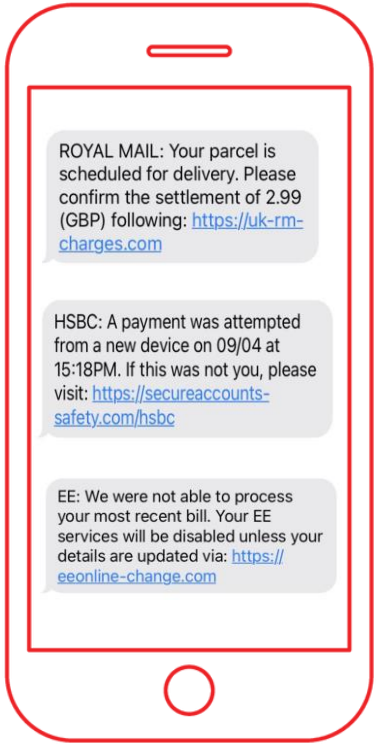
Phishing ist mittlerweile das **Cybersecurity-Risiko Nr. 1** weltweit und stellt häufig einen Einstiegspunkt für Angreifer dar.

85%

85% der Phishing-Angriffe auf mobile Endgeräte erfolgen außerhalb von E-Mails.

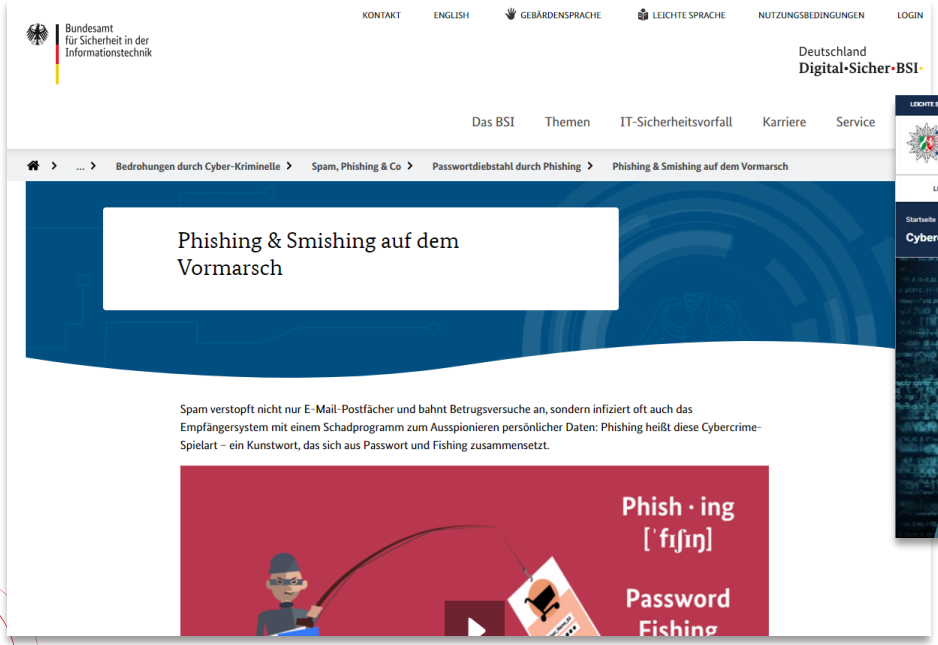
3x

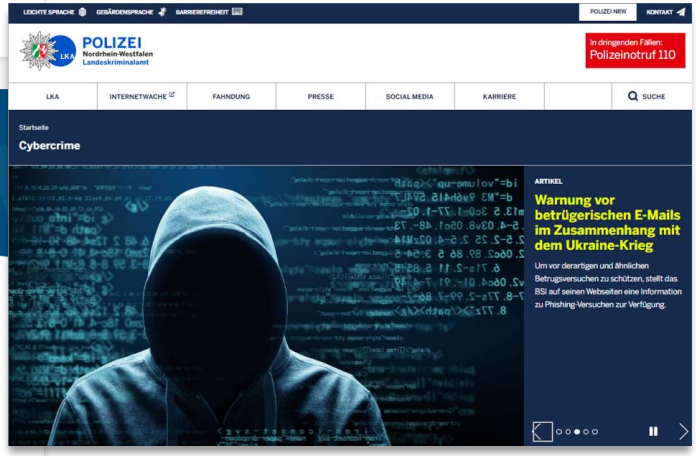
Lookout stellte fest, dass die **Wahrscheinlichkeit**, auf einen Phishing-Link zu klicken, auf dem **Handy 3x höher** ist als auf dem PC oder Desktop.



Aktuelle Lookout Fishing-Map hier
Aktuelle Lookout Threats-Map hier

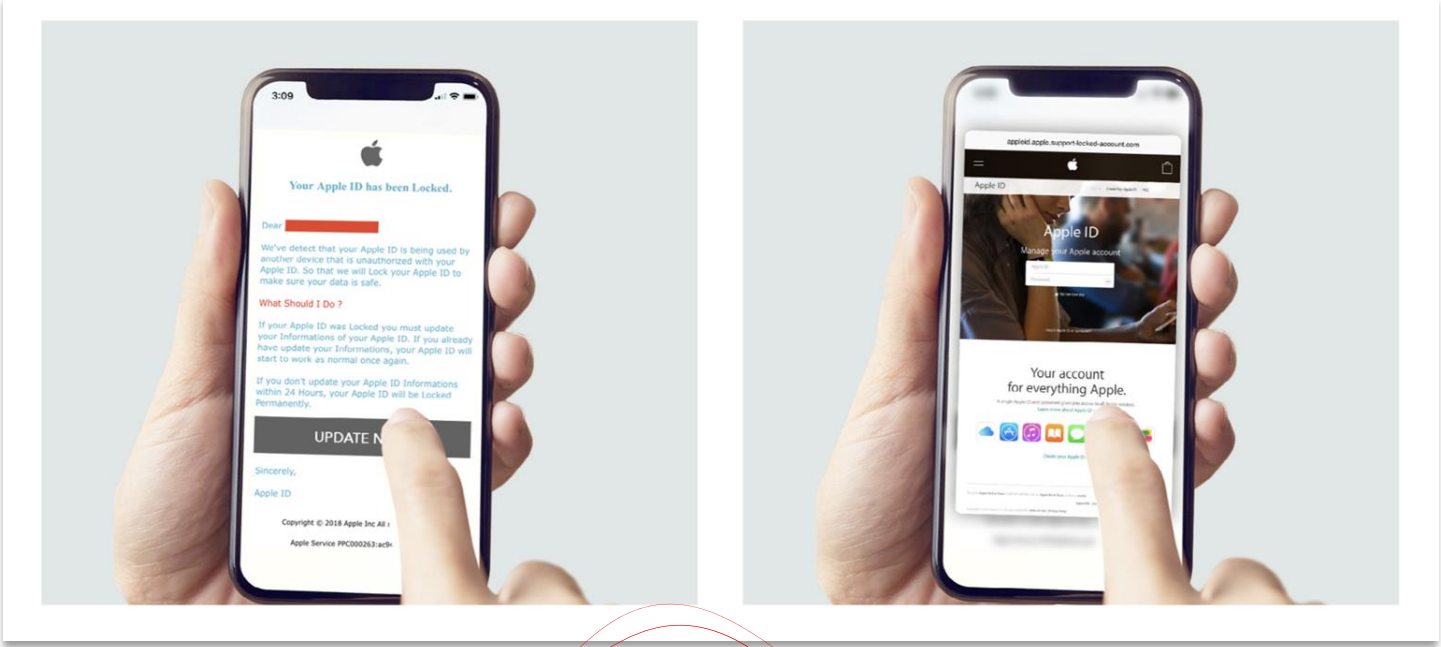
BSI & LKA warnen vor Smishing-Angriffen





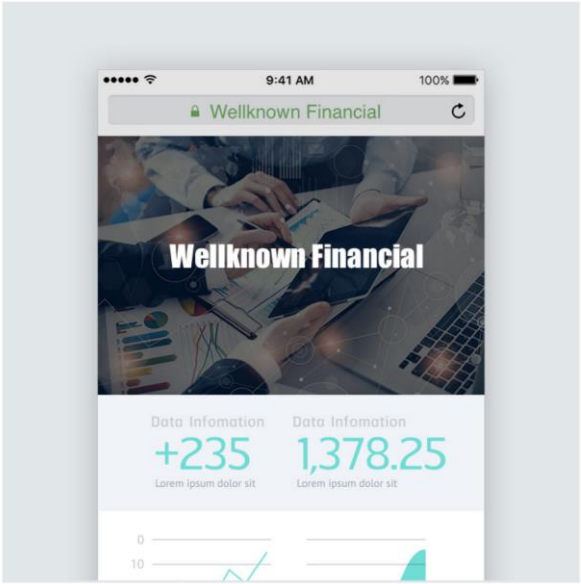
Was macht mobile Phishing-Angriffe so gefährlich?

1. Kein Link Hovering



Was macht mobile Phishing-Angriffe so gefährlich?

2. Fehlende URL-Visibilität & keine Möglichkeit, TLS-Zertifikate zu überprüfen



What's going on here: The address bar only shows the company name, not the actual URL

PC-Schutz ist schon umfassend da – mobile Geräte werden oft vernachlässigt

	APPS	DEVICE	NETWORK	WEB & CONTENT
PC	**Vom Unternehmen ausgewählt, gekauft und verwaltet** • Anti-Virus • DLP • Vulnerability scanning	**Vom Unternehmen ausgewählt, gekauft und verwaltet** • Verwaltung IT • Verwaltung SCCM • OS-Versionskontrolle • Überwachung der OS-Integrität • Verhaltensorientierte Überwachung	**LAN / Enterprise Wi-Fi VPN auf Reisen** • On device firewalls • Enterprise perimeter firewall	**Gefiltert am Unternehmensperimeter** • Secure Web Gateways
MOBILE	Von den Nutzer:innen ausgewählt, gekauft und verwaltet	COPE und BYOD Teilweise über EMM verwaltet	Immer auf dem Mobilfunknetz Von Nutzer:innen ausgewähltes Wi-Fi	Ungefiltert

Demo
Hacker-Angriffe

02

Angriff mit einer Phishing-Kampagne

Einsatz von Phishing-Werkzeugen

- Versehentliches Öffnen eines manipulierten QR-Codes
- Datendiebstahl über gefälschte Login-Website – zum Beispiel werden Zugangsdaten zu Office 365/Okta gestohlen

Ablauf Hacker-Angriff

Social Engineering

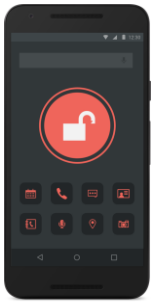
Über SMS, Textnachricht oder **QR-Code**

Malware installieren

- Spyware
- Surveillance
- Trojan/RAT
- Bösartiges Profil

Bösartige Seiten

- Datendiebstahl
- Zugangsdaten stehlen



Spionage

Senden und empfangen

- Daten, Bilder, Kamera, Audio
- Benutzerdaten

Angriff über die Stromzufuhr

Einsatz von „Juice Jacking“

- Unbemerkte Installation einer schädlichen Web App über Ladekabel, zum Beispiel am Flughafen oder im Zug
- Diebstahl der Zugangsdaten

Ablauf Hacker-Angriff

Gerät anschließen

Anschluss des Geräts an einen öffentlichen Ladeport

Gerät infiltrieren

Gefälschte Unternehmens-App installieren

Zugangsdaten stehlen

Nutzer:in öffnet versehentlich die gefälschte App und meldet sich an

Lookout & EMM

03

„Aber ich habe doch bereits eine EMM-Lösung!“

Enterprise Mobility Management – Die Haupteigenschaften

Mobile Device Management

- ✓ **Sicherheitsrichtlinien** durchsetzen
- ✓ **Geräte** sperren & Daten löschen
- ✓ Sperren von **Websites & Funktionen** wie Kamera
- ✓ VPN- & WLAN-Zugänge **zentral konfiguriert**

Mobile E-Mail Management

- ✓ **E-Mail-Zugang zentral** einrichten & auf Geräte pushen
- ✓ **Gefährdete Geräte** vom Zugriff auf Unternehmens-E-Mails **ausschließen**

Mobile Application Management

- ✓ **Kontrolle** über Installation von Apps
- ✓ **Apps verteilen**, schützen & nachverfolgen

Mobile Content Management

- ✓ **Zentrale Verwaltung** des Zugriffs auf **Unternehmensdaten** via SharePoint, OneDrive Pro, Dropbox
- ✓ Sicherer & einfacher **Zugriff**

Geräte-registrierung[1]

- ✓ **Vollautomatische** Konfiguration
- ✓ **Asset Protection:** Sicherung des Unternehmensbestands, Geräte nur im Unternehmenskontext einsetzbar

1) Bereitstellungsprogramm DEP von Apple und KME von Samsung

Die geschäftliche Nutzung von Geräten im Griff behalten

01

Ordnen Sie Geräte Ihrem **Unternehmen** zu – durch automatisierte Geräteausrollung

02

Profile können jederzeit **aus der Ferne aktualisiert** werden

03

Einhaltung der **Sicherheits-Richtlinien** zu Passwort-Konfiguration & Daten-Verschlüsselung

Transparenz & Kontrolle durch Echtzeit-Dashboards

Mit Lookout Advanced runden Sie Ihr EMM/MDM/UEMs ab.

Risiko Kategorien

	WEB + CONTENT	APPS	NETZWERK	ENDGERÄTE
Bedrohungen	• Phishing • Drive-by-download • Schadhafte Websites und Dateien	• Spyware und Überwachungssoftware • Trojaner • Schadhafte Apps	• Man-in-the-middle • Gefälschte Mobilfunkmasten • Root CA installation	• Privilege escalation • Remote Jailbreak/Root
SOFTWARE-SCHWACH-STELLEN	• Schadhafte Inhalte, die Schwachstellen im Betriebssystem oder in Apps auslösen	• veraltete Apps • Anfällige SDKs • Unzureichende Coding Praktiken	• Schwachstellen in der Netzwerk-Hardware • Sicherheitslücken im Protocol-Stack	• veraltetes OS • Dead-End-Hardware • anfällige vorinstallierte Apps
VERHALTEN & KONFIGURATIONEN	• Öffnen von Anhängen und Besuchen von Links mit potentiell unsicherm Inhalt	Apps, die • zu Daten-Verlust führen • Unternehmens-sicherheit verletzen • gegen Compliance verstoßen	• Proxies, VPNs, root-CAs • Automatisches einloggen in unverschlüsselten Netzwerken	• Von Benutzer:in initiierter Jailbreak/Root • Kein PIN Code/Password • USB debugging

Rot = kein Schutz durch EMM

Gelb = teilweise/ limitierter Schutz

Grün = Schutz durch EMM abgedeckt

Mit Lookout Schutz vor allen mobilen Angriffspunkten

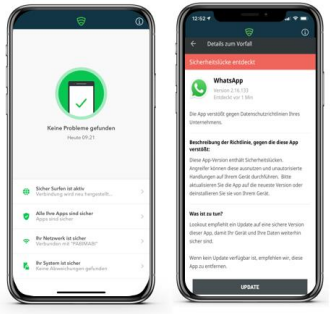
Verringern Sie das Risiko, dass Ihre **sensiblen Unternehmensdaten** durch einen **Sicherheitsvorfall** auf mobilen Endgeräten **preisgegeben** werden.

Schutz vor Web- und Content-Bedrohungen

- Phishing-Angriffe über persönliche und Firmen-konten via E-Mail, SMS, Messaging-Apps
- Schädliche oder bösartige Web-Inhalte
- Unangemessene Web-Inhalte, die gegen die Unternehmensrichtlinien verstoßen

Schutz vor Netzwerk-Bedrohungen

- Verbindung mit unsicheren externen Netzwerken
- Betrügerische WLAN-Netzwerke, über die Angreifer versuchen, Daten zu stehlen



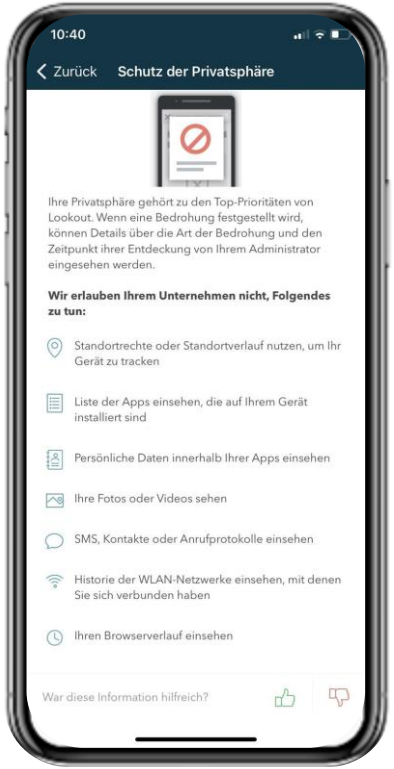
Schutz vor App-basierten Risiken

- Malware wie Spyware, Überwachungsprogramme oder Adware innerhalb von Anwendungen
- Datenlecks durch unsichere Anwendungen
- Anfällige Versionen von Anwendungen
- Außerhalb des offiziellen App-Stores heruntergeladene Apps

Schutz vor Geräte-Schwachstellen

- Veraltete Betriebssysteme ohne die neuesten Sicherheits-Patches
- Risiken bei der Gerätekonfiguration

Das Besondere an Lookout



- Lookout hat **keinen Zugriff** auf
  - Persönliche E-Mail-Inhalte
  - Browser-Verlauf
  - Textnachrichten oder andere persönliche Daten
- Lookout überprüft nicht den Inhalt von Nachrichten und **verletzt** daher **die Privatsphäre der Nutzer:innen nicht**
- Die **Datenschutzbestimmungen** werden **transparent** kommuniziert und sind für Benutzer:innen innerhalb der Lookout-Anwendung einsehbar
- Lookout verursacht **keinen übermäßigen Batterie- oder Datenverbrauch**

Wie schützt Lookout?

Management Konsole

Administrator:innen jeder Organisation kümmern sich um die mobile Sicherheit ihrer gesamten Flotte – über die webbasierte Lookout-Verwaltungskonsole.
Funktionen:

- Übersicht über Bedrohungen
- Einrichtung
- Sicherheitsrichtlinien

Lookout Security Cloud

Die Lookout Security Cloud nutzt das weltweit größte Mobil-Endgeräte-Netzwerk. So erkennt Lookout Bedrohungen **dank KI** – und schützt Nutzer:innen.

Lookout for Work App

Bis zu 90% der Bedrohungen beheben Benutzer:innen mit der schlanken Lookout-App auf dem Endgerät selbst.
Funktionen:

- Warnung vor Bedrohungen
- Einfache Schritte zur Behebung
- Datenschutzinformationen

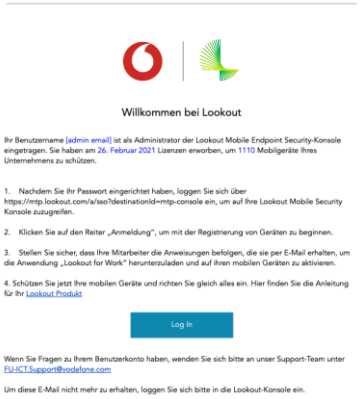
Unternehmens-ressourcen geschützt

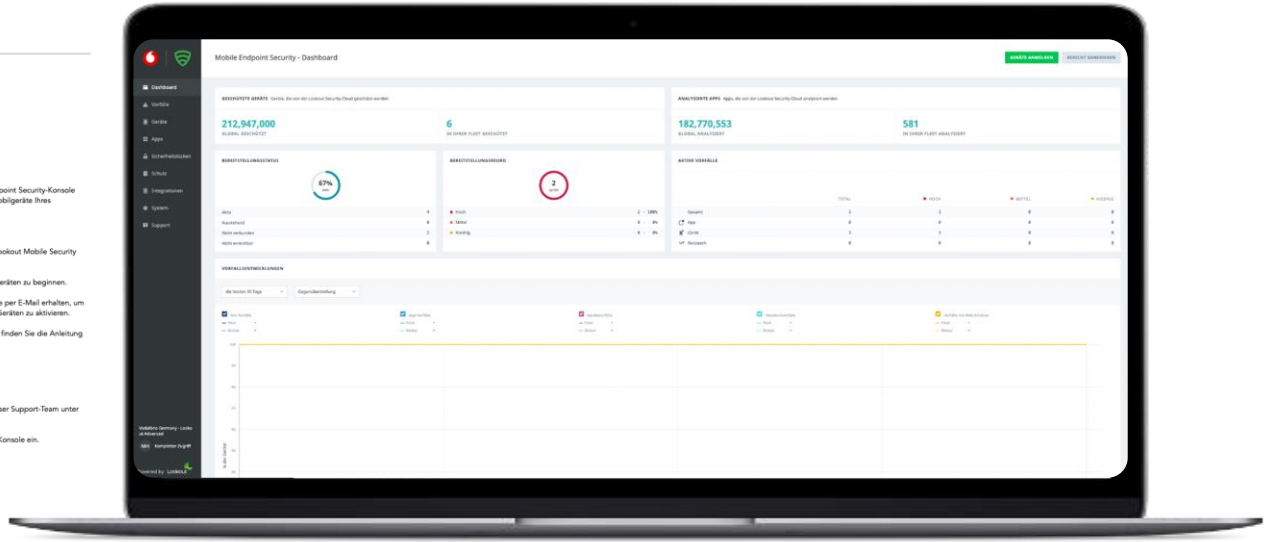
Sie greifen sicher auf Unternehmensdaten zu und ermöglichen so flexibles Arbeiten.

Lookout Konsole

Einfacher Rollout von Lookout Advanced

Aktivieren Sie den Schutz Ihrer mobilen Geräte in wenigen Schritten.





Manuelle Aktivierung via Adminkonsole erforderlich –
Rollout auch über Ihr EMM/UEM/MDM möglich.

Ihr Vorteile mit Lookout im Überblick.

Zusammenfassung

Mobile Sicherheit ist entscheidend für jedes Unternehmen

4%

der Unternehmen geben an, dass sie bereit sind, mit einem Angriff auf das Mobiltelefon umzugehen.

41%

der Lookout-Benutzer:innen wurden innerhalb der ersten 90 Tage über eine mobile Bedrohung informiert.

85%

der Benutzer:innen öffnen bösartige URLs auf mobilen Endgeräten. Dieser Anteil steigt seit Jahren.

Vorteile auf einen Blick

- Einfache Einrichtung & Nutzung
- Lookout greift nicht auf persönliche Infos zu
- Beeinflusst die Leistung von Endgeräten nicht
- Unterstützt von weltweit größter Threat Intelligence-Datenbank
- Deckt Sicherheits-Anforderungen für einen Mix aus COPE- und BYOD-Endgeräten ab

IHRE FRAGEN.

Vielen Dank für Ihre Teilnahme!

Bei Fragen
melden Sie sich gern
bei Ihrem:r Vodafone-
Ansprechpartner:in.

Sie sind neu bei uns?
Schreiben Sie uns an
online.sessions@vodafone.com
eine E-Mail.

Aufzeichnungen der
Online-Sessions
aus unserem Educational
Month Cyber Security
finden Sie hier oder im
Content Hub.


Together we can
vodafone
business