nomasis
secures your mobility

Smartphones im Polizeieinsatz: Zwischen Dienstgerät und Privatnutzung

spik
SWISS POLICE ICT

MOBILE SECURITY 20 YEARS

26.03.2025

Inhalt

- Einleitung ins Thema
- Bedrohungen und Risiken
- Nutzung im Polizeialltag
- Technische Massnahmen für Hybridlösung
- Ungelöste Themen
- Diskussion

Über uns

Martin Tanner

Leiter Systemtechnik
ICT
Stadt Polizei Zürich

Philipp Klomp

Gründer und CEO
Nomasis AG

Nutzung im Polizeialltag – Stadtpolizei Zürich

- Alle Mitarbeiter erhalten ein geschäftliches iPhone
- Unterschiedlicher Zugriff auf diverse «Polizei-APP's»
- Nutzung privat und geschäftlich
- Erreichbarkeit ausserhalb Bürozeit (Alarmierung)

Nutzung im Polizeialltag – Stadtpolizei Zürich

- Motorräder / Fahrzeuge werden mit iPhone/iPad ausgerüstet.
- Funktioneller Zugriff auf spezifische «Polizei-APP's»
- Nutzung nur geschäftlich möglich und fix verbaut
- Zusammenarbeit mit der Einsatzzentrale (Disposition, Ortung, Zielnavigation)

Immer mehr Business Content

Unified Communication
- Email, Attachments, Kontakte, Termine, Aufgaben
- Instant Messaging, Videokonferenz und Telefonie

Mobile Webapplikationen
- Intranet, ERP, CRM, Sharepoint, HTML5 Content
- Native App Verbindung ins Unternehmen

Dokumente
- PDF, Word, Excel, Präsentationen, Fileshares
- Textverarbeitung, Multimedia

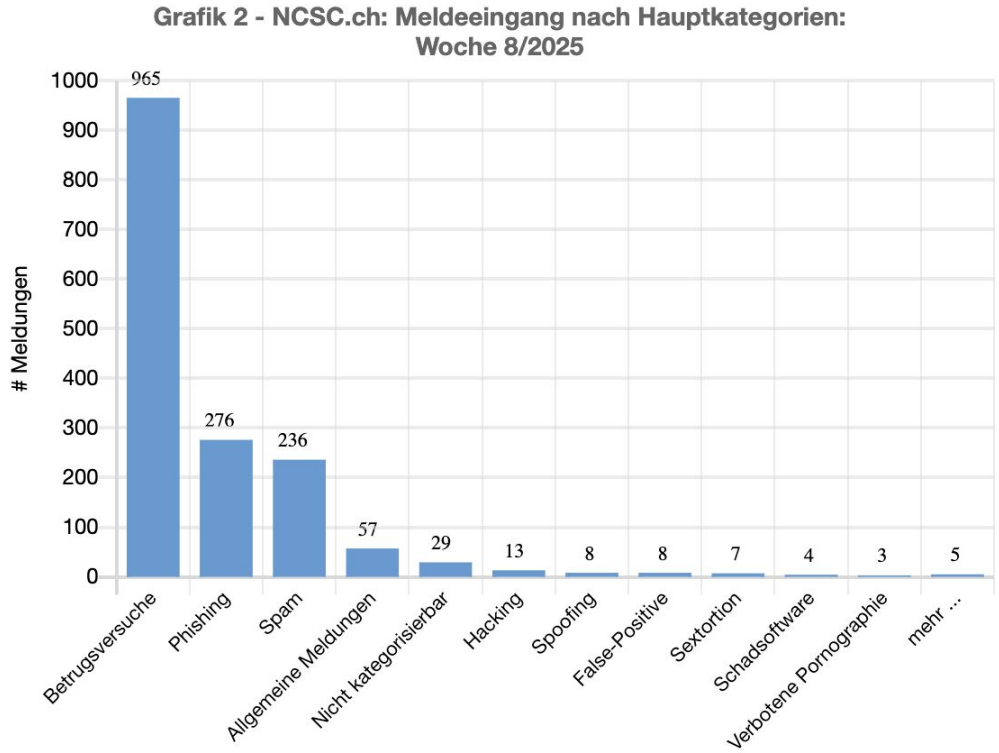
Selber entwickelte Polizei-Apps
- Informationen, Bestellungen, Prozesse, Erfassungen
- Zentrales Rollout und App Management

Trust Anker
- MFA, Mobile ID
- Location / VPN Services

Das Handy in unserem Leben

- Bezahlungen
- Online Banking
- E-Mail, Kalender, Telefon
- SMS, Social Media
- Unterhaltung (Filme, Spiele)
- Schlüssel (Auto, Haus, PC)
- Foto und Videokamera
- Hotspot / Access Point
- Sport / Gesundheit
- Lernen / Wissen
- Reisen / Ticketing
- Und vieles mehr …

Aktuelle Bedrohungslage



Quelle: ncsc.ch

Situation in der Schweiz

netzwoche NEWS STORYS DOSSIERS VIDEO SPECIAL

NEWS

Whatsapp-Mods als Einfallstor

Cyberangriffe auf Smartphones und Tablets nehmen zu

Di 27.02.2024 - 09:51 Uhr
von Joël Orizet und msc

Angriffe auf mobile Geräte haben im vergangenen Jahr weltweit um über 50 Prozent zugenommen. Allein in der Schweiz gab es über 60'000 Cyberangriffe auf Smartphones und Tablets. Häufige Einfallstore sind der Google Play Store sowie Whatsapp- und Telegram-Mods.

netzwoche

NEWS STORYS DOSSIERS VIDEO SPECIALS EVENT

NEWS

Notfallupdate verfügbar

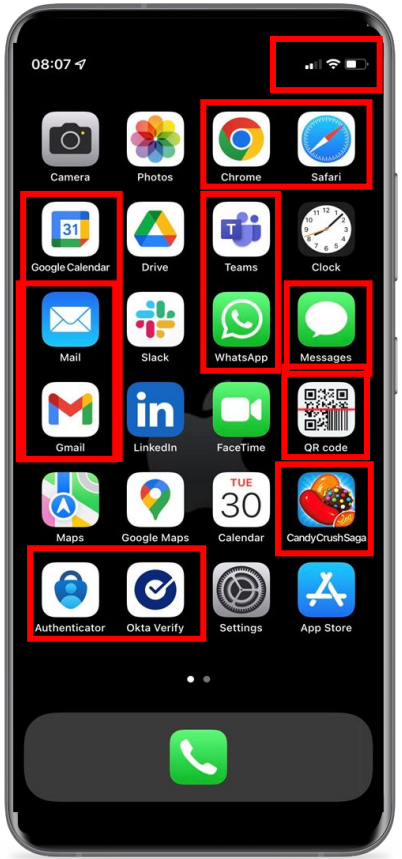
Zero-Day-Schwachstelle bei Apple ermöglicht iPhone-Hack

Do 05.10.2023 - 12:31 Uhr
von Maximilian Schenner und cka

Eine Zero-Day-Sicherheitslücke gefährdet iPhone- und iPad-User. Die Schwachstelle erlaubt es Angreifern, ihre Rechte am Gerät auszuweiten. Apple stellte ein Notfallupdate bereit.

Welches sind die Angriffspunkte?

Netzwerk	Ungesicherte WiFi-Netzwerke oder Hotspots
Apps	Persönliche und Unternehmens-Apps
	Apps, die Daten preisgeben oder übertragen
	Fremde App Stores oder schädliche Anwendungen
Web & Inhalte	Schädliche Webinhalte
	Phishing-Angriffe
	Scannen von QR-Codes
Gerät	Veraltete Betriebssysteme



Smartphone wird schwaches Glied

Wenig Investitionen für Smartphone Sicherheit in den letzten Jahren

Smartphone ist wesentliches Glied für Cloud Security (MFA)

MDM ist eine Verwaltung und keine volle Sicherheitslösung

Risiken und Bedrohungen zu wenig bekannt / priorisiert

Mögliche Lösungen

- 1 Gerät Privat und Geschäft oder 2 Geräte
- Mobile Threat Defense Lösung (Virenschutz)
- Einschränkungen für private Nutzung (Supervised)
- Trennung geschäftliche und private Daten (Getrennte Apple ID und Apps)
- Klare Rechte und Pflichten für Mitarbeiter und Arbeitgeber
- Haftungsklauseln
- Schulung / Awareness

MTD & MDM im Vergleich

	WEB & INHALT	APPS	NETZWERK	GERÄT
THREATS	Phishing	Bösartige Anwendungen	Man-in-the-middle	Advanced Jailbreak/Root
SOFTWARE SCHWACHSTELLEN	Schwachstellen im Betriebssystem	Veraltete Anwendungen	Schwachstellen in der Netzwerkhardware	**Veraltetes Betriebssystem**
VERHALTEN & KONFIGURATIONEN	Öffnen von Anhängen	Apps, die Daten abziehen	Automatische Verbindung zu unverschlüsselten Netzen	Kein Pin-Code/Passwort

Durch MDM abgedeckt | Teilweise mit MDM | Nur mit MTD

Das MTD System ist die halbe Miete…

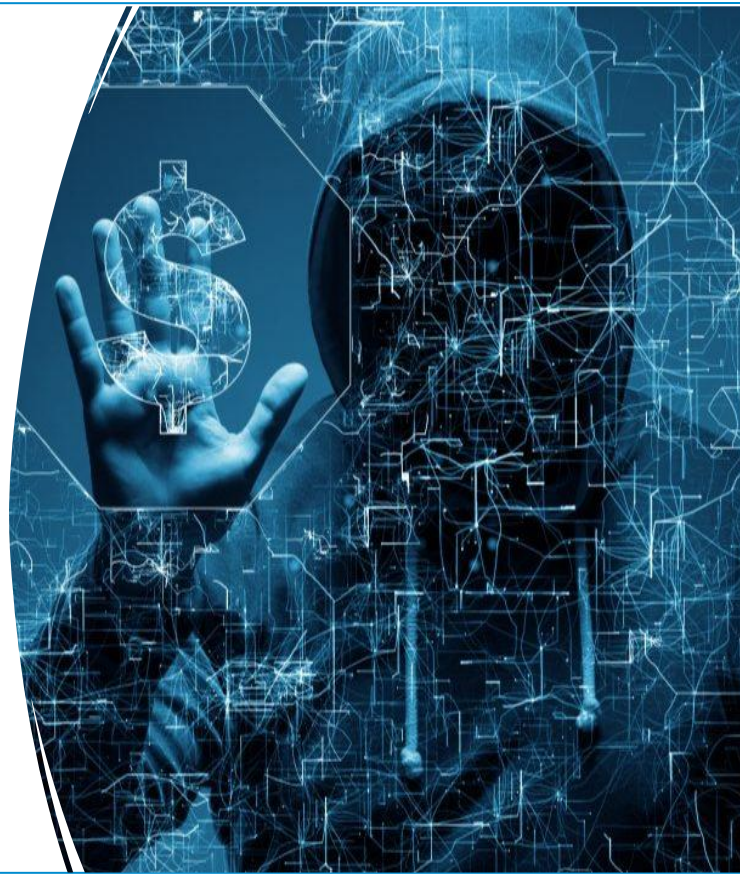
- Integration ins SOC/SIEM / Sicherheitsprozesse
- Einbezug der Smartphone Benutzer
- Security Playbooks für mobile Geräte
- Nomasis Mobile SOC Service

Ungelöste Themen

- Cloud Themen (Privat und Geschäft). Z.B Apple Cloud Polices versus Microsoft
- App Entwicklung und regelmässige App Überprüfung auf Schwachstellen
- Option 2 Geräte anstelle 1 Gerät (Work Life Balancing)
- Inhaltbasierte Sicherheit

Fazit

- Smartphone wird immer mehr zur Identität / Trust Anker
- Das persönliche und geschäftliche Leben ist auf dem Smartphone
- Trennung Privat und Polizei ist nicht einfach lösbar
- Es besteht Handlungsbedarf in Bezug auf die Sicherheit
- Nomasis bietet MTD und Mobile SOC Lösungen



Sie finden uns am Stand 18

- Gemeinsam mit unseren Security Partnern