nomasis
secures your mobility

Wieso Unternehmen ihre Smartphones und Tablets schützen sollten

Februar 2024

Nomasis AG • Spinnereistr. 12 • CH-8135 Langnau a. A. • info@nomasis.ch • +41 43 377 66 55 • www.nomasis.ch

Wieso Unternehmen ihre Smartphones und Tablets schützen sollten

Von Patrick Trevisan – Mobile Security Consultant – Nomasis AG

Seit Jahrzehnten schützen Unternehmen ihre PCs und Laptops mit Antivirenprogrammen, Firewall-Einstellungen, VPN-Verbindungen und anderen Schutzmechanismen. Bei Smartphones und Tablets vertrauen sie weiterhin auf die Betriebssystem-Architektur und auf Mobile Device Management Systeme, obwohl die meisten Attacken auf Unternehmensdaten, -infrastrukturen und Individuen heutzutage bei Smartphones und Tablets beginnen.

Mobile Threat Defense (MTD) Lösungen für Smartphones und Tablets gibt es bereits seit rund 20 Jahren auf dem Markt und bieten Schutz gegen Phishing, Netzwerkattacken, App-Risiken und anderen Bedrohungen. Aber die meisten Unternehmen investieren erst in eine solche Versicherung, wenn es zu spät ist.

Smartphones und Tablets: Ein offenes Scheunentor für Angreifer

Apple und Android Smartphones und Tablets haben schon seit einigen Jahren Einzug in Unternehmen genommen und im Rahmen von 'Modern Work' und 'Arbeiten von überall' nimmt die Anzahl stetig zu. Sei es lediglich für die Synchronisation von E-Mail, Kalender und Kontakte aber auch für den Zugriff auf CRM, SAP, Firmenapplikationen und weitere Dienste, stellen diese Geräte in der modernen Arbeitswelt mittlerweile ein unverzichtbares und effizientes Arbeitsmittel dar.

Dies haben natürlich auch böswillige Angreifer erkannt. Einerseits befinden sich auf diesen Geräten eine Vielzahl von Informationen wie Passwörter, Kreditkarten, Informationen über Personen und Unternehmen sowie weitere für Spionage und kriminelle Aktivitäten nützliche Daten. Andererseits sind auch Zugriffe auf Kamera, Mikrofon und andere Sensoren keine filmreife Utopie mehr, wie jüngste Angriffe auf namhafte Unternehmen und Institutionen aufzeigen.

Dabei gilt es ebenfalls zu beachten, dass Unternehmen den privaten Einsatz ihrer Smartphones und Tablets erlauben oder eine Bring-Your-Own-Device (BYOD) Strategie fahren. Dies erhöht den Angriffsvektor um ein Vielfaches, da zum Beispiel Phishing-Attacken auch von privaten E-Mails, SMS und Apps an das Gerät gelangen können.

Umso mehr erstaunt es, dass viele Unternehmen immer noch davon ausgehen, dass sie mit einem Mobile Device Management (MDM) System und der Betriebssystemarchitektur von Apple iOS/iPadOS und Google Android genügend geschützt sind. Sie realisieren nicht, dass Smartphones und Tablets ohne entsprechende zusätzliche Sicherheitsmassnahmen, die schwächsten Glieder in ihrer Geräteflotte darstellen und latente Angriffsvektoren für Kriminelle darstellen.

MDM Systeme verwalten mobile Geräte und bieten lediglich IT Grundschutz

Ein MDM System ermöglicht die einfache Einbindung, Inventarisierung und Verwaltung von mobilen Geräten. MDM stellt zwar eine gute und wichtige Basis für den Betrieb und der Absicherung von mobilen Geräten in Unternehmen dar, bietet aber einen sehr tiefen Grundschutz bezüglich IT-Sicherheit. Dieser IT Grundschutz beschränkt sich nämlich auf folgende Funktionen:

- Forcierung eines Geräte PINs resp. Biometrie
- Rudimentäre Sicherheitsrichtlinien bezüglich OS Versionen
- Rudimentäre Richtlinien bezüglich App Blacklisting
- Richtlinien bezüglich Data Loss Prevention
- Schutz vor Jailbreaks/Root Zugriffe welche vom Anwender initiiert werden

MDM Systeme bieten keinen Schutz gegen folgende Risiken:

- Phishing Attacken
- Schadsoftware
- Sideloading von Apps
- Apps mit schwachem oder böswilligem Code
- Netzwerkattacken (z. Bsp. Man-In-The-Middle)
- Versteckte Jailbreaks/Root Zugriffe
- Früherkennung von neuen Bedrohungen

Das Android und iOS/iPadOS Betriebssystem ist sicher… oder doch nicht?

Schaut man sich die Statistiken über erfolgte Angriffe und Angriffsvektoren mal genauer an, realisiert man schnell, dass auch Apple und Google stets beschäftigt sind, Vulnerabilitäten und Sicherheitslöcher in ihren Betriebssystemen und App Frameworks zu schliessen.

Genauso wie Microsoft für Windows, erscheinen für iOS und Android von Apple und Google regelmässige Sicherheitsupdates und Hotfixes, welche Sicherheitslücken schliessen und neue Funktionalitäten, um die Sicherheit zu gewährleisten, einbauen.

Ebenso muss man beachten, dass sich besagte Plattformen meistens ausserhalb des Unternehmensperimeters befinden und sich mittels unbekannten WiFi- oder Datennetzverbindungen zu den Unternehmensdaten verbinden. Darüber hinaus befinden sich heutzutage viele Daten-Backends in der Cloud, was zusätzlicher Kommunikationssicherheit auch auf mobilen Geräten bedarf.

Nachfolgend Statistiken von cvedetails.com zu den einzelnen Geräteplattformen und deren bekannten Vulnerabilitäten:

Google Android

Vulnerabilities by types/categories

Year	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	File Inclusion	CSRF	XXE	SSRF	Open Redirect	Input Validation
2014	1	0	1	0	0	0	0	0	0	0	1
2015	60	53	0	0	0	0	1	0	0	0	6
2016	85	47	0	0	0	0	0	0	0	0	47
2017	190	95	0	0	1	0	0	0	0	0	61
2018	145	158	3	0	2	0	0	1	0	0	49
2019	41	181	4	0	1	0	0	0	0	0	34
2020	103	223	9	0	6	0	0	0	0	0	68
2021	74	202	2	0	5	0	0	0	0	0	51
2022	104	342	5	0	11	0	0	0	0	0	97
2023	122	342	2	0	4	0	0	0	0	0	64
2024	3	22	0	0	0	0	0	0	0	0	0
Total	928	1665	26		30		1	1			478

Quelle und weitere Details

Apple iPhone OS

Vulnerabilities by types/categories

Year	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	File Inclusion	CSRF	XXE	SSRF	Open Redirect	Input Validation
2014	35	43	0	1	1	0	0	2	0	0	10
2015	184	196	0	0	5	0	1	3	0	0	26
2016	84	99	0	3	0	0	0	0	0	0	10
2017	210	205	0	14	0	0	0	0	0	1	30
2018	55	53	0	1	0	0	0	0	0	1	13
2019	82	182	2	14	0	0	0	0	0	0	48
2020	22	106	0	8	2	0	0	0	0	0	20
2021	23	98	0	6	3	0	0	0	0	1	7
2022	16	81	0	0	0	0	0	1	0	0	4
2023	15	26	0	1	0	0	0	0	0	0	2
2024	1	7	0	0	0	0	0	0	0	0	0
Total	727	1096	2	48	11		1	6		3	170

Quelle und weitere Details

Apple iPad OS

Vulnerabilities by types/categories

Year	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	File Inclusion	CSRF	XXE	SSRF	Open Redirect	Input Validation
2014	0	0	0	0	0	0	0	1	0	0	0
2019	0	21	0	1	0	0	0	0	0	0	2
2020	21	84	0	5	2	0	0	0	0	0	14
2021	21	83	0	6	3	0	0	0	0	1	7
2022	16	73	0	0	0	0	0	1	0	0	3
2023	16	24	0	1	0	0	0	0	0	0	1
2024	1	7	0	0	0	0	0	0	0	0	0
Total	75	292		13	5			2		1	27

Quelle und weitere Details

Mobile Threat Defense (MTD): Der konkrete IT Schutz für mobile Geräte

Wie eingangs erwähnt, gibt es auf dem Markt seit jeher Lösungen, welche die Bedrohungen für mobile Geräteplattformen genauso gut schützen, wie die Lösungen, welche wir schon immer auf PCs und Laptops einsetzen. Diese Lösungen werden Mobile Threat Defense oder kurz MTD genannt und bieten komplementäre IT-Sicherheit für mobile Geräteplattformen bezüglich folgender Risiken und Einstiegspunkte:

- Netzwerk
  - Ungesicherte WiFi-Netzwerke oder Hotspots
  - Man-In-The-Middle Attacken
- Apps
  - Persönliche und Unternehmen-Apps
  - Apps, die Daten preisgeben oder übertragen
  - Side-Loading oder schädliche Apps
  - Schlecht codierte Apps
  - Veraltete Apps
- Web & Content
  - Phishing Angriffe
  - Scannen von QR-Codes
  - Schädliche Webinhalte
- Gerät
  - Versteckte Jailbreaks und Root Access
  - Veraltete Betriebssysteme
- Früherkennung von neuen Bedrohungen in allen Bereichen

Solche MTD-Lösungen basieren grundsätzlich auf einer Machine-Learning Datenbank und scannen regelmässig Millionen von Geräten und Apps ohne die Privatsphäre der Anwender zu verletzen, erkennen Anomalien und können, je nach konfigurierter Sicherheits- oder Interventionsrichtlinie, entsprechende Massnahmen wie Sperren von Zugriffen bis hin zu Ausserdienststellung des Gerätes auslösen.

Die meisten Lösungen bieten darüber hinaus eine Integration mit bestehenden MDM-, IAM- und SIEM-Infrastrukturen. So kann auch die mobile Geräteflotte sicherheitstechnisch von SOC-Mitarbeitern überwacht und wenn nötig eingegriffen werden.

Die Nomasis schützt Sie, Ihre Endbenutzer und Ihre Geräteflotte im Rahmen ihres Nomasis Mobile Threat Defense Management Services in Zusammenarbeit mit namhaften MTD Herstellern. Klicken Sie hier für weitere Informationen.