Der AirBorne Apple AirPlay-Sicherheits-Hack Angekündigt am 29. April 2025:

Was bedeutet dies für die IT-Sicherheit in Schulen ?

Am 29. April 2025 enthüllten Cybersicherheitsforscher von Oligo Security den AirBorne-Hack, eine Reihe von Schwachstellen im AirPlay-Protokoll von Apple. Diese Schwachstellen ermöglichen Remote Code Execution (RCE) mit Zero-Click-Interaktion und können jedes AirPlay- oder AirPlay-kompatible Gerät in einem WLAN-Netzwerk zu einem angreifbaren Host machen.

Weitreichende Wirkung über AirPlay-Geräte hinaus

Die AirBorne-Sicherheitslücken betreffen nicht nur die geschätzten 2,5 Milliarden AirPlay-fähigen Geräte, sondern auch alle Geräte, die drahtloses Casting über das AirPlay-Protokoll unterstützen. Dazu gehören Millionen von Fernseher, interaktive Flachbildschirme (IFPs) in Klassenzimmern, netzwerkfähige Kameras, intelligente Lautsprecher und Mikrofone. Viele dieser Geräte, insbesondere moderne interaktive Bildschirme (IFPs) großer Hersteller, sind AirPlay-kompatibel und stellen somit potenzielle Angriffspunkte für Angreifer dar.

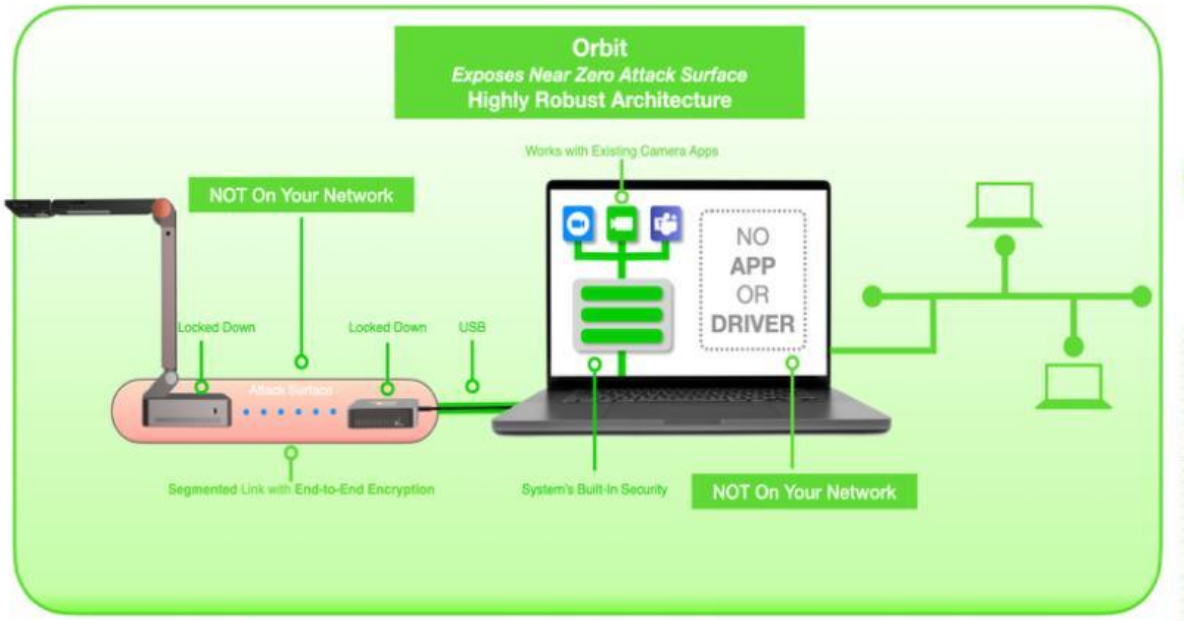
Unterstützen IFP's in Ihrer Schule oder Ihrem Schulbezirk AirPlay?

Kompromittierte Geräte können zu Abhör- oder Überwachungsinstrumenten werden und stellen ein erhebliches Risiko für sensible Daten wie Schülerinformationssysteme (SIS) oder andere vertrauliche Aufzeichnungen in Schulnetzwerken dar. Wenn Ihr Schulbezirk AirPlay-kompatible Geräte verwendet, ist es wichtig, sich umgehend an Ihre Anbieter zu wenden und sich nach Sicherheitspatches zu erkundigen.

Orbit-Kameras: Eine sichere Alternative

Wenn Sie eine drahtlose Orbit Pro- oder Orbit Air-Kamera verwenden, können Sie beruhigt sein – diese Geräte sind vom AirBorne-Hack nicht betroffen. Warum? Orbit-Kameras arbeiten mit einer segmentierten Netzwerkarchitektur und sind daher vom WLAN Ihrer Schule isoliert. Der Orbit-Empfänger-Dongle, der über einen USB-Anschluss oder HDMI-Eingang angeschlossen wird, fungiert als physische Firewall.

Dadurch entsteht ein geschlossenes Netzwerk (siehe Seite 2), das ausschließlich mit der gekoppelten Kamera über einen einzigartigen, werkseitig festgelegten Verschlüsselungsschlüssel kommuniziert. Diese Verbindung ist durch eine Ende-zu-Ende-AES-256-Verschlüsselung gesichert, wodurch sichergestellt wird, dass Video- und Audiostreams geschützt bleiben.



Im Gegensatz zu anderen Geräten, die auf offene Netzwerkdienste angewiesen sind, vermeiden Orbit-Kameras unnötige Netzwerkexpositionen und sind daher ein weniger attraktives Ziel für Angreifer. Im Gegensatz dazu bieten in Ihr WLAN integrierte Geräte einen breiteren Zugriff, vergleichbar mit einer unverschlossenen Hintertür, während das isolierte Netzwerk von Orbit wie ein befestigtes Eingangstor wirkt.

Warum der AirBorne-Hack nicht überraschend ist:

Die AirBorne-Sicherheitslücken verdeutlichen ein umfassenderes Problem:
Proprietäre Software in Ihrem Netzwerk kann versteckte Risiken bergen. Selbst Apple, ein weltweit vertrauenswürdiger Hersteller mit Milliarden von Geräten, hat versehentlich Sicherheitslücken in seinem AirPlay-Protokoll hinterlassen. Dies wirft Fragen zu anderen weit verbreiteten Technologien auf. Schließen die häufigen Updates von Microsoft ähnliche Sicherheitslücken? Ist Miracast sicher? Was ist mit den Smart-Apps auf Ihren interaktiven Bildschirmen? Diese sollten untersucht werden.

Warum die HoverCam-Orbit heraussticht:

Orbit-Kameras – sowohl die Pro- als auch die Air-Modelle – bieten robuste Sicherheit ohne Kompromisse bei der Funktionalität. Im Gegensatz zu Konkurrenzprodukten benötigt Orbit keine Treiber oder Apps und gewährleistet so echten Plug-and-Play-Betrieb, ohne Ihre Netzwerkkonfiguration ändern zu müssen. Durch die Sperrung von Kamera und Empfänger-Dongle schützt Orbit die interne Sicherheit, sodass Sie sich auf den Schutz Ihres Netzwerks konzentrieren können.

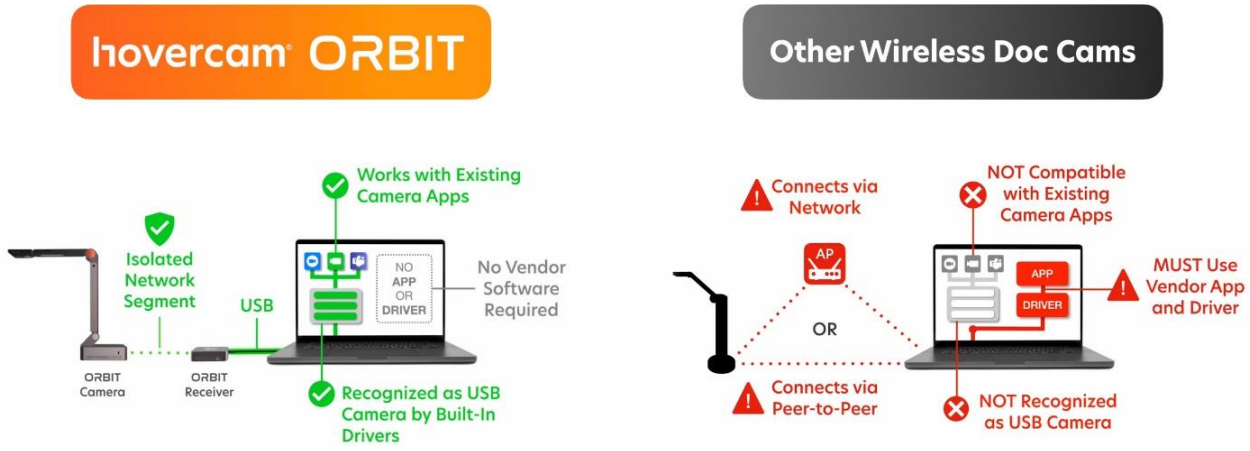
Die Orbit Pro geht einen Schritt weiter und nutzt das 60-GHz-Frequenzband – im Gegensatz zum 5-GHz-Band herkömmlicher WLAN-Geräte. Dadurch ist das Signal des Pro für herkömmliche Internetgeräte unsichtbar und bietet zusätzlichen Schutz: Angreifer können nichts angreifen, was sie nicht erkennen können.

Der Wert der Sicherheit von Orbit:

Orbit-Kameras kosten etwas mehr als einige Konkurrenzprodukte. Das liegt am integrierten, hochentwickelten Empfänger-Dongle, der als natürliche Firewall fungiert und die Sicherheit vor Bedrohungen wie dem AirBorne-Hack erhöht. Der Aufpreis sorgt für ein beruhigenderes Gefühl und gewährleistet, dass Ihre Geräte in einer zunehmend anfälligen digitalen Landschaft geschützt bleiben.

Wenn Ihr Bezirk auf AirPlay-kompatible Geräte angewiesen ist, prüfen Sie jetzt bitte die Patches der Anbieter. Für alle, die eine sichere Alternative suchen, bietet die isolierte, verschlüsselte Architektur von Orbit einen sicheren Schutz gegen netzwerkbasierte Angriffe.

Vergleich der HoverCam Orbit zu anderen drahtlosen Kameras im Netzwerk:



Weitere Informationen zur Sicherheitsarchitektur von Orbit mit animierten und vertonten Beschreibungen finden Sie auch unter

https://www.hovercam.com/orbit/security.