Enterprise-Hardware

Das, was eine Firma will, sobald sie realisiert hat, dass sie kein Consumer ist. (Kein Scherz)

- Transition und Eingliederung neuer Kunden
- Lenovo == IBM
- Drucker
- sicherer Apple Geräte-Transport
- Sophos
    - Sophos Webfilter / WebPortal

Transition und Eingliederung neuer Kunden

Nie direkt durchgeführt, also nur reines theoretisches Doing:

Hardware

- Welche externe Internetanbindung liegt an? Wie schnell ist diese?
- Kann der eingesetzte Router die Geschwindigkeit überhaupt unterstützen?
  - Richtwerte: Vodafone EasyBox und Lancom (8xx Serie): max bei 250 Mbit/s IPsec, etwas schneller bei Cleartext-Internet
- Kann die eingesetzte Firewall die Geschwindigkeit auch im Realtimescan unterstützen?

Wenn alles bis hier hin überwiegend mit "Nein" beantwortet wird, sind wir pro Standort schon bei mindestens 1500-2000€ reiner Hardwarekosten. Man braucht vielleicht keine Gigabit-scanning Firewalls, aber hier sollte man besonders bei vorhandenem Mixing verschiedener Hersteller auf Einheitlichkeit achten.
Auch wenn es doof klingt: Ein Forti-Router mit Forti-Firewall ist besser als ein Lancom-Router der eine Forti-Firewall füttert.
Klar hat man dann umso kritischere RCE-Lücken bei Einheitlichkeit, aber man hat bessere Interoperabilität.

Hier also weiter mit:

- Router raus, Firewall raus
- ausreichende Firewall mit Routingfunktion direkt an ISP ran. Neues zentrales Management hochziehen.

Software

oft der viel längere Part, weil es hier direkt in Richtung Datenschutzverträge geht. Nicht mehr so viel darum welche Software geeignet ist. Apple hat z. B. nichts Vergleichbares wie Azure.

- Was setzt der Kunde aktuell gerade ein?
- Wie viele Softwarehersteller sind im Ernstfall beteiligt?

Hier wieder Einheitlichkeit. Alles mit PowerApps gebastelt ist auf den ersten Blick billig, resultiert aber zwangsmäßig in recht statischen Systemen (nicht jeder kann PowerApps und dank Fachkräftemangel kann man nicht davon ausgehen, dass ein Mitarbeiter bleibt. Muss bedacht werden). Zwiespalt hier ist wieder, dass sich PowerApps-Geklicke dynamisch anpassen lässt,

während man bei Atlassian (oder welchen Hersteller es auch immer trifft) eher die Workflows anpassen muss. Das widerspricht dem deutschen Typ Gewohnheitstier ganz deutlich.
Einheitlichkeit: Wenn Jira für Tickets, dann auch Confluence für Team-Management. Wenn schon Exchange Online, dann auch Office Lizenzen im gleichen Tenant. Das ist überhaupt kein Problem mehr, weil es Gerätegebundene Apps for Enterprise Lizenzen gibt. Wenn schon Exchange Online, dann bitte auch Azure AD und keine Onprem-ADs wieder (übrigens ist auch ein im Dienstleister-Haus gemietetes AD onprem - nur eben die Cloud vom Dienstleister).
Vertraulichkeitsverträge mit Microsoft, nicht mit dem Dienstleister. Der Dienstleister kann euch dabei unterstützen, den Vertrag mit Microsoft zu erreichen. - Der sollte euch aber kein Dienstleister-Onprem andrehen - (tut er oft mit "Sie kommen ja in UNSERE Cloud"). Ja, Onprem heißt vor-Ort, und das wäre es auch mit Dienstleister nicht mehr, aber ich würde das dann auch nicht mehr als Cloud bezeichnen.

Lenovo == IBM

Titel sagt alles.

Enterprise-Mäßig ist Lenovo-Hardware fast 1:1 IBM. Jeder hat des anderen Produkte auf den eigenen Markennamen gelabelt...

Consumer ist unterschiedlich, bzw. ist die Enterprise-Sparte von Lenovo aus IBM übernommen.

Drucker

Printserver

seit 2021 nur noch packaged V4 Usermode drivers

Nach PrinterNightmare hat Microsoft den Download von Druckertreibern, die sich Clients vom Printserver laden können ein auf Type 4 Benutzermodus Treiber beschränkt. Auch "package aware" Treiber genannt: A Practical Guide to PrintNightmare in 2024 | itm4n's blog

Microsoft hat also 2021 Treiber sprichwörtlich auf V4 Benutzermodus begrenzt.

non-package-aware drivers wird man auch weiter über andere Softwareverteilungsmethoden installiert bekommen, fällt damit aber ein Schritt vom Komfort eines Printservers wieder zurück.

Hersteller

Eigentlich ein verhasstes Thema. Dennoch machen auch viele Hersteller nur noch Murks mit ihren Treibern.

Ich breche das hier mal auf in Druck, Scan als WIA und Scan als TWAIN. Druck ist in der Regel gegeben, Scan oftmals nicht.

NAPS2 ist das scanning-Programm. Steuert NAPS2 die MFPs nicht richtig an, fließt das hier direkt in die Bewertung rein. TWAIN und WIA sind Standards, daher liegts an deren Implementierung im Druckertreiber, ob daraus Murks gemacht wurde oder nicht.

HP

völlig umgehen. Die Treiber folgen gar keinen Standards. Nicht einmal die Windows Installer Bibliotheken. TWAIN und WIA sucht man vergebens beim Scannen...

- Keine Windows Update Treiber
- kein WIA
- kein TWAIN

Triumph Adler

- Keine sauberen Treiber von Windows Update, also kein volles Plug&Play.
- Printing geht mit Windows Update, die muss man aber, wenn man Scannen möchte, wieder runterhauen, weil...
- TWAIN Scanning benötigt non-WHQL Printing-Treiber von der Homepage.

- Länderspezifische Treiber? TA in AT für gleiche Modelle andere Treiber als TA in DE?

Alles in allem eher suspicious...

Lexmark

am problemfreiesten bisher. Benötigt extra Treiber für TWAIN, die aber dank automatischer Druckererkennung relativ idiotensicher sind und vor allem sowohl sauberes WIA als auch sauberes TWAIN sprechen.

- Drucktreiber vorinstalliert: ja
- Scantreiber vorinstalliert: nein
- WIA: ja
- TWAIN: ja

Xerox

- hat prinzipiell einen Imageschaden bekommen - setze ich mich also gar nicht erst mit auseinander.

sicherer Apple Geräte-Transport

> TL;DR - nur Apple kann dauerhafte Gerätesperren setzen, für eine dauerhafte Gerätesperre benötigt Apple die Geräte-Verknüpfung zu einer Apple ID.
> MDM-Gerätesperren sind ab MDM-Entfernung aufgehoben was genau das Ziel der Diebe ist.

Voraussetzungen

- Apple Business Manager
- Händler, welche Geräte vorregistriert
- Händler, welcher Freigabeprozesse zwischen Vorregistrierung und Versand ermöglicht
- MDM mit Profilen (z.B. Intune)

Doings

1. Klassische Apple ID anlegen (z.B. transportdevices@company.com)
2. MDM profil anlegen, enforcing der Apple ID auf iOS
3. Shop bitten Geräteregistrierung zu machen
4. Geräte im Apple Business Manager zum MDM server hinzufügen
5. MDM profil für neu registriertes Gerät setzen
6. Freigabe zum Versand erteilen

Reaktion bei ordnungsgemäßem Empfang

1. Vor erstem Anschalten das MDM-Profil ändern
2. Gerät einsetzen

iPhone Prozess bei Dieb

1. Dieb oder Käufer der Hehlerware schalten das Gerät ein
2. Einrichtungsprozess kann durchgangen werden
3. Dieb sorgt für Internetzugriff, durch SIM oder WLAN
4. Im Einrichtungsprozess wird keine Möglichkeit gegeben eine Apple ID anzugeben
5. Die durch das MDM Profil vergebene PIN ist aktiv
6. Durch die Apple ID können die Geräte von Apple selbst verwaltet werden, weil Apple den MDM Herstellern weniger Zugriff gestattet.
   (z.B. Komplett-Deaktivierung des gesamten Geräts, auch nach Entfernung aus MDM)

Nachsorge nach Diebstahl

Voraussetzung: Dieb oder sein Käufer muss das Gerät eingeschaltet haben. Sieht man im MDM.

- Als Apple ID transportdevices@company.com mit Apple kommunizieren.
- Apple über Diebstahl und polizeiliche Anzeige aufklären.
- Anzeige erstatten
- Polizei den Umstand mit der Apple ID erklären
- Polizei Zugriff auf eure transportdevices Apple ID geben. (Geolokation über "Wo ist" Netzwerk)
- Nach Bestätigung von Apple und Zeitablauf der Anzeige dass dieses Gerät komplett deaktiviert wurde aus dem MDM entfernen.

Die meisten Anzeigen werden nicht weiterverfolgt, da es sich nicht um Diebstähle in großem Maß handelt und die Jurisdiktion von Polizeiarbeit über Ländergrenzen hinweg deutlich schwieriger ist.

Warum?

Apple erlaubt ohne Apple ID keine dauerhafte Gerätesperre.
Das Ziel der Diebe ist nicht das iPhone, sondern der Erlös des Verkaufs von diesem.

Der Hehler hat keine Kundschaft, wenn er Geräte verkauft die für seine Kunden nicht einsetzbar sind, und fordert demzufolge auch keine neuen Geräte vom Dieb an.

Drittanbieter-MDM's können keine dauerhaften Gerätesperren setzen! Auch Intune ist in der Hinsicht Drittanbieter.
Dauerhaft bedeutet ein kompletter Soft-Brick der Geräte. Egal nach welcher Methode, diese Seriennummer hat keine Betriebserlaubnis bei Apple mehr...

Wie kann der Dieb mit den Geräten umgehen?

- SMD-Lötstation haben
- Zugriff auf Spare-Part-Chips aus gleicher Modellserie haben
- SMD-Chip auslöten und anderen einlöten

Dies ist ein Prozess der fast ausschließlich nur im Produktionsland der iPhones gemacht werden kann.
Die Endpunkte der Hehlereiware sind in der Regel nicht die Produktionsländer.

Quirks and Features

- Mit eurem MDM hat Apple nichts zu tun

- Apple kann erst Geräte sperren, wenn sie Internetverbindung hatten, und eine Apple ID auf dem Gerät aktiv war
- Über das Enforcing der Apple ID sorgt ihr dafür dass ein Apple Device ab dem ersten einschalten im "Wo ist" Netzwerk von Apple ist.

Sophos

Sophos Webfilter / WebPortal

Login To Network Funktion

Wenn ihr die Login To Network Funktion nutzt, funktioniert die Aktivitätserkennung ("Tab offen lassen") via Javascript... Wenn der Browser crasht oder der Prozess hart beendet wird, läuft die JavaScript Action fürs Tab Schließen nicht und der komplette Rechner bleibt vom Webfilter ausgenommen...

Ob es einen serverseitigen Timeout gibt muss ich noch testen...

Weitere Ansätze:
MAC Address Spoofing anderer Geräte die bereits freigegeben sind etc...