CASESTORY

Erasmus Universiteit

Inhoud

Mobiele devices zijn overal

Het gebruik van mobiele devices heeft de afgelopen jaren een grote vlucht genomen. Even snel een e-mail beantwoorden, PDF document bekijken of een eetafspraak inplannen; mobiele devices zijn naadloos geïntegreerd in ons leven.

Zo ook het studerende en werkende leven. Onderzoekers, studenten en medewerkers maken op grote schaal gebruik van mobiele apparatuur zoals smartphones en tablets bij het delen en vergaren van informatie. Daarbij is het vrijelijk delen van de juiste informatie een essentieel onderdeel.

De academische wereld is divers en internationaal georiënteerd. Nog belangrijker dus dat gegevens veilig, snel en compleet onderling kunnen worden gedeeld en er goed kan worden samengewerkt.

Mobiele toestellen, security en cybercrime

Dit introduceert echter ook beveiligingsvraagstukken voor toegang, ontsluiting en gebruik van toepassingen en online data. Zo vrij toegankelijk is de informatie nu ook weer niet natuurlijk.

Met geavanceerde mobiele hacks zoals de Pegasus software kan zonder medeweten van de gebruiker software op het toestel worden geïnstalleerd en daarmee toegang tot de mobiele gegevens worden verkregen. Een ander voorbeeld is de Universiteit van Maastricht die in 2019 volledig werd platgelegd door een cyberaanval.

Opleidingsinstellingen, universiteiten en hogescholen waren en zijn dus gewaarschuwd.

Beveiliging en het onderwijs: de Erasmus Universiteit

Zo ook de Erasmus universiteit. Naast alle maatregelen die de Security afdeling al onderneemt heeft het beveiligen van de mobiele devices (smartphones en tablets) de bijzondere aandacht. Zoals zoveel onderwijscentra maakt ook Erasmus van de Microsoft online omgevingen gebruik. Het online benaderen van gegevens gebeurt met smartphones, laptops, tablets en dergelijke. In dat kader maakt de Erasmus universiteit gebruik van de Microsoft Endpoint Manager om haar eindpunten te beveiligen. Eigen apparatuur, dus in het bezit van de Erasmus universiteit zelf, is naar eigen inzichten te beveiligen en is daarmee onder controle te brengen en te houden.

BYOD: persoonlijk vs werk

Een grotere uitdaging is het beveiligen van Bring Your Own Device (BYOD) apparatuur, in het bezit van de eindgebruiker zelf. Deze apparatuur is, zoals gezegd, in privé bezit en bevat dus persoonlijke informatie van de gebruiker.

Om gebruikers in staat te stellen om met eigen apparatuur ook gegevens van de EUR te benaderen moeten er speciale maatregelen genomen worden. Zo moet de gebruiker 100% gegarandeerd worden dat zijn persoonlijke gegevens niet door de Erasmus universiteit ingezien kunnen worden. Daarnaast moet Erasmus er ook zeker van zijn dat haar gegevens beschermd kunnen worden conform haar eigen beveiligingsbeleid. Verder zal de gebruiker zeker moeten weten dat hij te allen tijde de zakelijke beveiliging kan verwijderen zonder enige gevolgen voor het eigen toestel.

Indien niet aan deze eisen kan worden voldaan, dan zal er geen vertrouwen van de gebruiker zijn om het eigen toestel in te zetten voor online gegevensbenadering. Het alternatief is dan dat gebruikers een toestel van de zaak willen gebruiken en dus met meerdere toestellen over straat moeten. Ook niet ideaal.

BYOD: Microsoft Intune, Android en iOS onder controle

Om het BYOD vraagstuk te tackelen is het belangrijk om te weten welke mogelijkheden de industrie te bieden heeft. Er is sprake van een samenspel van leveranciers en service providers, zoals Microsoft, Google, Apple en system integrators die deze werelden met elkaar kunnen verbinden.

Zo biedt Google met Android Enterprise de oplossing voor moderne op Android gebaseerde apparatuur. Apple heeft met haar eigen Device Enrollment en User enrollment alternatieve security oplossingen voor BYOD. Microsoft verrijkt dit met de mogelijkheden die Intune biedt als onderdeel van de Microsoft Endpoint Manager, zoals Mobile Application Management (MAM) en Conditional Access (CA).

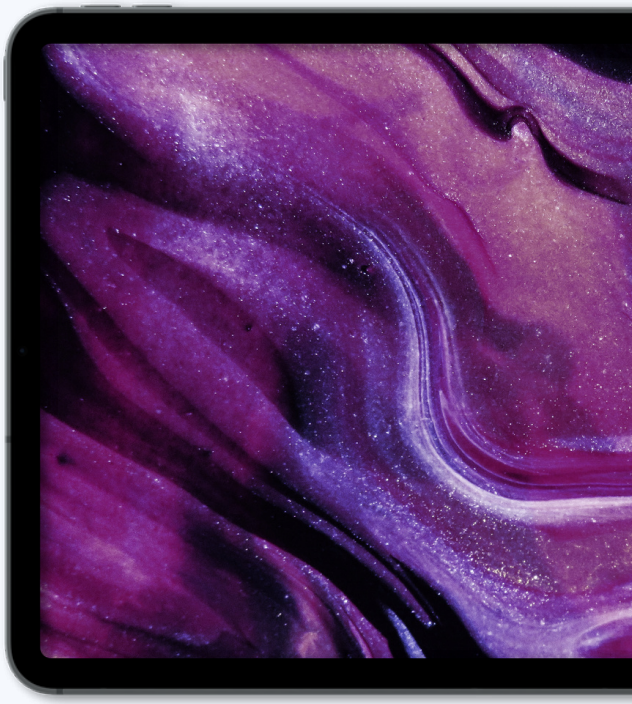
Het samenspel van Microsoft, Google en Apple geeft de Erasmus universiteit de mogelijkheid voor het realiseren van een goed werkbare BYOD oplossing waarmee werk gegevens optimaal van persoonlijke gegevens gescheiden kunnen worden zonder een inbreuk te doen op het eigen toestel.

BYOD: het Android Werkprofiel en Mobile Application Management

Android biedt met het Android Enterprise (ook wel bekend als 'Android for Work') een zeer uitgebreide en veilige oplossing voor diverse 'use cases'. De use case voor BYOD maakt gebruik van het zogenaamde 'Werkprofiel' concept. Hierbij installeert een gebruiker een Werkprofiel (container software) waarvan de inrichting en de beveiliging geheel onder controle staat van de IT afdeling. Dit Werkprofiel wordt automatisch gevuld met de applicaties die door de Erasmus universiteit beschikbaar worden gesteld. Een gebruiker hoeft zelf geen applicaties te installeren en weet zeker dat de werkgegevens ook veilig binnen het werkprofiel zijn ondergebracht.

Om de gebruikerservaring optimaal te ondersteunen zijn er mogelijkheden om gegevens uitwisseling tussen het persoonlijke profiel en het werkprofiel toe te staan. Hiermee kan aan de individuele wensen en behoeften van gebruikers tegemoet gekomen worden zonder concessies voor de beveiliging.

Apple biedt met User enrollment als onderdeel van Apple MDM een vergelijkbare functionaliteit, deze hebben echter de status preview bij Microsoft. Voor Apple wordt daarom van de Mobile Application Management (MA)M voorziening van Microsoft gebruik gemaakt om beveiliging op applicatieniveau af te dwingen.



BYOD: Werkprofiel en online leven naast elkaar

De Erasmus Universiteit maakt gebruik van het Android Werkprofiel voor de BYOD Android gebruikers. Dit impliceert dat gebruikers een inrichting van het Android Werkprofiel moeten doen op hun eigen apparatuur voordat er van de Erasmus werkomgeving gebruik kan worden gemaakt. Niet alle gebruikers willen dit of hebben behoefte aan de volledige werkomgeving. Men wil bijvoorbeeld alleen even de e-mail raadplegen en hebben dan geen behoefte aan het werkprofiel. In dat geval kan er online gewerkt worden of is er de optie van MAM waarbij de alleen de Outlook applicatie wordt beveiligd op het eigen toestel.

BYOD beveiligen: 'the way to go'

Om de gebruikers er van te overtuigen dat de bedachte BYOD oplossing veilig is en dat de persoonlijke gegevens van de eindgebruikers gewaarborgd zijn en die van de werkgegevens afgeschermd, moet er goede- en helder afstemming met de eindgebruikers plaatsvinden. Dit vraagt om het in -kaart brengen van de huidige werkwijze van de gebruikers, welke typen BYOD toestellen worden er ingezet, wat is het beleid dat van toepassing is op de BYOD inrichting en het commitment van het management/CISO/CvB etc.

Hiervoor zijn een aantal, voor de EUR representatieve-, gebruikers (friendly users) geselecteerd die in een kleine gecontroleerde Microsoft intune omgeving met de voorgestelde beveiliging aan de slag gaan. Hun ervaringen worden opgetekend, teruggekoppeld en verwerkt om zodoende tot een baseline inrichting te komen voor de mobiele BYOD toestellen. Zaken als minimale OS versie die wordt toegestaan, uitzonderingssituatie, installatie-instructies en documentatie, betrokkenheid van de supportdesk en de IT beheerafdeling, communicatieplanning, uitrolplanning en afstemming met alle partijen komen uitgebreid aan de orde.

De uitrol vindt op een gefaseerde en gecontroleerd wijze plaats waarbij operationele bevindingen in het rollende traject worden ingebracht. Daarbij is gebruikgemaakt van de additionele mogelijkheden die Application Management van Microsoft te bieden heeft voor een fijnmazige inrichting van Microsoft applicaties. Hierdoor wordt de oplossing voor gebruikers steeds meer op maat gesneden en wordt de gebruikerstevredenheid nauwgezet gevolgd.

Het resultaat: BYOD veilig en tevreden gebruikers

De Erasmus universiteit beschikt na de uitrol van het mobiele beveiligingsbeleid over een goed werkende BYOD oplossing voor persoonlijke Android toestellen. Gebruikers moeten een Werkprofiel op hun Android toestel installeren en hebben minimaal Android versie 9 nodig om toegang te krijgen tot hun Erasmus gegevens. De uitrol heeft op een beheerste en gefaseerde wijze plaatsgevonden waardoor gebruikers de kans hebben gekregen hun opmerkingen en verbetervoorstellen gedurende het traject in te brengen. Door de snel te verwerken en aanpassingen door te voeren wordt voor een goede gebruikerservaring gezorgd. Dit wordt als heel prettig ervaren en biedt de basis voor een gezonde en veilige werkplek voor de mobiele gebruikers van de Erasmus Universiteit.

Meer weten?

Wilt u meer weten over het verbeteren van Mobile Security? Cloud Seven biedt een geïntegreerde benadering voor het beter beveiligen van mobiele endpoints. Neem contact op en start het gesprek met onze specialisten. Bezoek ook onze website: www.cloudseven.nl

Contactgegevens

+31 (0)79 363 4250

m.kuiken@cloudseven.nl

Bleiswijkseweg 37F, 2712 PB Zoetermeer