Auteurs: Vincent van Dijk en Chris de Vries. Vincent van Dijk is eigenaar van Security Scientist en is bereikbaar via vincent@securityscientist.net. Chris de Vries is redacteur van het IB Magazine en daarnaast eigenaar van De Vries *Impuls* Management, hij is bereikbaar via impuls@euronet.nl.

Hoe beveilig je een Mac laptop?

HULPGIDS BEVEILIGING VOOR HET KLEINBEDRIJF (DEEL 4)

In het vorige artikel hebben we uitgebreid gekeken naar het beveiligen van Windows-laptops en -computers. Maar wat als je een Mac-laptop gebruikt? In dit artikel zullen we dieper ingaan op de beveiliging van Mac-laptops en hoe je ervoor kunt zorgen dat je apparaat beschermd blijft tegen bedreigingen.

Zijn Mac-laptops veiliger? Dat wordt veelal gedacht en dan heb je waarschijnlijk gelijk. Op het gebied van malware hadden Mac-systemen, in 2020, maar 75.000 malware detecties tegenover 111 miljoen malware detecties bij Windows systemen (1). Deze getallen zeggen nog niet zoveel omdat hierin geen rekening is gehouden met de veel grotere hoeveelheid Windows-systemen die in omloop zijn in verhouding tot Mac-systemen. Volgens de statistieken draait 74,48 procent van alle laptops en desktops op een Windows-systemen en slechts 16,67 procent op Mac-OS (2). Dat betekent 4.450 malware detecties per 1 procent marktaandeel voor Mac en 1,49 miljoen malware detecties per 1 procent marktaandeel voor Windows.

Mac-systemen (b)lijken dus daadwerkelijk veiliger of zij worden in elk geval minder aangevallen

Zit het verschil dan misschien in de gebruikers van de Mac-laptops? Creatieve professionals, zoals grafisch ontwerpers en videobewerkers gebruiken de Mac voor hun artistieke projecten. Ondernemers en *tech-savvy* professionals vertrouwen op de betrouwbaarheid en integratiemogelijkheden met andere Apple-producten voor een soepel Apple-ecosysteem. Allemaal op dezelfde hardware aangeleverd door Apple.

Aan de andere kant hebben Windows-laptops ook een brede gebruikersbasis, en zij trekken vaak gebruikers aan die waarde hechten aan diverse hardware-opties. Windows-laptops zijn populair onder zakelijke professionals vanwege de beschikbaarheid van een scala aan software en hardware die op Windows draait.

Zou het soort gebruiker invloed hebben op de lagere dreiging van de Macbooks?

De Mac lijkt wel een stuk veiliger te zijn, maar dat betekent niet dat je geen rekening hoeft te houden met betrekking tot de beveiliging van jouw Mac-laptop! Net zoals bij Windows bestuderen we bij de beveiliging van jouw Mac-systeem drie thema's, te weten:

- Hygiëne
- Veilige configuratie
- Systeemkennis

Hygiëne

Net als bij Windows-laptops is het ook bij Mac-laptops belangrijk om regelmatig opruiming te houden. Verwijder onnodige bestanden, programma's en tijdelijke gegevens die opslagruimte in beslag nemen en prestaties vertragen. Dit doe je door regelmatig de door jou geïnstalleerde applicaties door te nemen en ongebruikte programma's te verwijderen. Gelukkig is dit bij Mac een stuk makkelijker en kan je via de 'applicaties' folder al jouw applicaties inzien en gemakkelijk verwijderen. Daarnaast adviseren wij: maak gebruik van de ingebouwde tool 'Opslagbeheer' om tijdelijke bestanden en andere overbodige gegevens te verwijderen.

Tegenwoordig creëren wij ook veel chaos binnen en met onze webbrowsers. Webbrowsers slaan tijdelijke bestanden, cookies en browsegeschiedenis op. Dat beïnvloedt de prestaties en brengt de privacy en security in gevaar. Het opschonen van de browser verloopt voor Mac- en Windows-laptops via eenzelfde route. Zorg ervoor dat je regelmatig de cache en cookies van de browser leegt en de browsegeschiedenis verwijdert om jouw browse-ervaring fris en veilig te houden. Bekijk ook de instellingen van de browser om extensies te beheren en verwijder onnodige of verouderde add-ons. Ons advies: installeer twee belangrijke add-ons met betrekking tot de browser:

1. UBlock Origin - een adblocker die virussen blokkeert die via advertenties verspreid worden. Vermijd andere adblockers, aangezien deze een reputatie hebben om virussen te bevatten. Zie ook ons voorgaand artikel in dit magazine (3).
2. Cookie Auto Delete - zorgt ervoor dat de cookies van jouw webbrowser(s) netjes opgeruimd worden.

Naast het opruimen van onnodige bestanden is het cruciaal om sterke wachtwoorden en een wachtwoordbeheerder te gebruiken om wachtwoorden veilig op te slaan. Als je volledig in het Apple-ecosysteem zit, gebruik dan eventueel de password manager van Apple (ICloud keychain). Een persoonlijke mening: concentreer niet al jouw sleutels op één plek en benut dus een aparte passwordmanager, zoals Bitwarden. Zie ook hier ons vorig artikel (3).

Veilige configuratie

Macbooks worden geleverd met ingebouwde beveiligingsfuncties die je kunt activeren om jouw systeem te

beschermen. Meestal staan deze functies al aan, maar toch is het goed om de functies nog even te controleren. Hier zijn enkele stappen die je kunt nemen:

1. zorg ervoor dat jouw Mac-OS up-to-date is door regelmatig de software-updates te installeren. Dit gaat automatisch, maar veel Mac-gebruikers herstarten niet vaak genoeg de laptop om de updates door te voeren;
2. activeer de ingebouwde firewall op jouw Mac om ongeautoriseerde toegang tot jouw systeem te voorkomen. Ga naar 'Systeemvoorkeuren' > 'Beveiliging en privacy' > 'Firewall' en zet de firewall aan;
3. gebruik FileVault om de gegevens te versleutelen. FileVault is een ingebouwde encryptiefunctie op de Mac waarmee je de volledige harde schijf kunt versleutelen en
4. activeer de 'Gatekeeper'-functie om te voorkomen dat je ongewenste software installeert. Ga naar 'Systeemvoorkeuren' > 'Beveiliging en privacy' > 'Algemeen' en kies voor 'App Store en geverifieerde ontwikkelaars'.

Bekijk naast deze features ook de 'privacy & security'-instellingen van jouw laptop. Met een Mac specificeer je namelijk per applicatie de te gebruiken features. Zo gebruik ik (Vincent) Firefox voor het dagelijks browsen; deze browser heeft geen camera of microfoon toegang. Moet ik dan toch videobellen over de browser, dan gebruik ik expliciet de Chromebrowser die toegang tot deze features heeft.

Eén van de toegangen, welke vaak even gecontroleerd moet worden, is de 'Full Disk Access'. Eigenlijk moeten nagenoeg alle applicaties geen '**álle** bestanden'-toegangsrechten bezitten. Hetzelfde geldt voor 'file access'. Controleer bij file access of de applicaties geen toegang hebben tot folders die ze eigenlijk niet nodig hebben.
Ook net zoals bij de Windows-systemen is het goed om een onderscheid te maken tussen een gebruikers- en een administratieve account. Met een apart beheerdersaccount en een standaardgebruikersaccount verminder je de kans dat schadelijke software of malware wordt geïnstalleerd zonder dat je het weet. Het standaardgebruikersaccount heeft geen toegang tot belangrijke systeeminstellingen en systeembestanden, waardoor het minder vatbaar is voor onbedoelde wijzigingen die het systeem kunnen beschadigen.
Om een standaard (niet-admin) account aan te maken op een Macbook, volg je deze stappen:

1. ga naar het Apple-menu (linksboven in de menubalk) en selecteer: 'Systeemvoorkeuren';
2. klik in het venster 'Systeemvoorkeuren' op 'Gebruikers en groepen';
3. klik op het hangslotpictogram in de linkerbenedenhoek van het venster en voer het beheerderswachtwoord in om wijzigingen aan te brengen;
4. klik op het plusteken (+) onderaan de lijst van gebruikers om een nieuwe gebruiker toe te voegen;
5. kies bij het drop-down menu 'Nieuwe account' voor 'Standaard';
6. vul de vereiste velden in voor de standaardgebruiker, zoals de volledige naam en een accountnaam. en
7. klik op de knop 'Maak aan'.

Systeemkennis

Mac is net even wat anders gestructureerd dan Windows. Het is goed om dat verschil te zien, want dan begrijp je ook waarom alles anders functioneert bij Mac dan bij Windows, dus ook security.

Mac en Windows zijn twee verschillende besturingssystemen die worden gebruikt op computers. Mac-OS is het besturingssysteem dat wordt ontwikkeld door Apple en is exclusief ontworpen voor Apple-computers, zoals Macbooks en iMacs. Het is gebaseerd op de Darwin-kernel, die afstamt van UNIX, en deelt daarom bepaalde kenmerken met UNIX, zoals een op UNIX-gebaseerd bestandssysteem en een UNIX-terminal genaamd 'Terminal'.

Aan de andere kant wordt Windows ontwikkeld door Microsoft. Het is beschikbaar voor een scala aan computers van verschillende fabrikanten. Het maakt gebruik van de Windows NT-kernel, die een ander ontwerp en een andere

functionaliteit heeft dan de Darwin-kernel. Het verschil in hardware zorgt ervoor dat Mac minder kwetsbaar is met betrekking tot hardware bedreigingen, maar met als nadeel dat Mac minder types hardware ondersteunt.

Wat toegangsbeheer betreft heeft Mac-OS vaak een strenger beleid dan Windows. Mac-OS gebruikers moeten vaak hun wachtwoord bevestigen wanneer ze bepaalde systeemwijzigingen willen aanbrengen, wat een extra beveiligingslaag biedt. Windows-gebruikers hebben niet altijd dit niveau van toegangscontrole. Ondanks dat Windows hier wel zeker verbeterslagen aan het maken is, merk je dat de Mac dat vanuit de *core* echt wat beter voor elkaar heeft - veel van de Linux-principes zijn hier overgenomen.

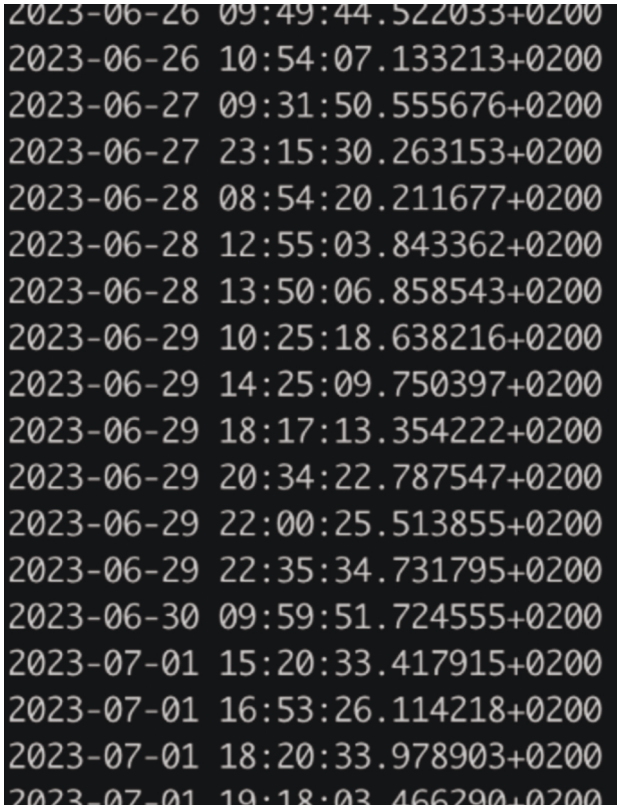
Logging werkt bij OSX echt even anders dan bij Windows. Je hebt niet een mooie interface waar je lekker door de logs heen kunt scrollen. Daarnaast zijn de logs ook minder toegankelijk. Om de logs te doorzoeken moet je de terminal leren te gebruiken. Via het commando 'sudo logs show' lees je de logs uit.

Als voorbeeld: met het commando 'sudo logs show\' zie je wanneer jouw laptop toegankelijk is/was (dus de 'unlock' functie geactiveerd is/was). Dit is handig als je vreest dat iemand fysiek heeft ingebroken op jouw laptop. Na toepassing van het commando zie je alle databestanden die via jouw laptop toegankelijk zijn geweest.

```
sudo log show --style syslog  --last 1d | awk '/Enter/ && /unlockUIBecomesActive/ {print $1 " " $2}'
```

Om de logs te bekijken moet je wel eerst de terminal openen. Om de terminal te kunnen openen moet je de volgende stappen doorlopen:

1. Zoek de 'Terminal'-applicatie. Ga naar de map 'Hulpprogramma's' in de map 'Programma's';
2. Dubbelklik op de 'Terminal'-applicatie: klik twee keer op het 'Terminal'-icoontje om de terminal te openen en
3. de terminal wordt geopend: je ziet een venster met een opdrachtregel waarin je commando's kunt typen.

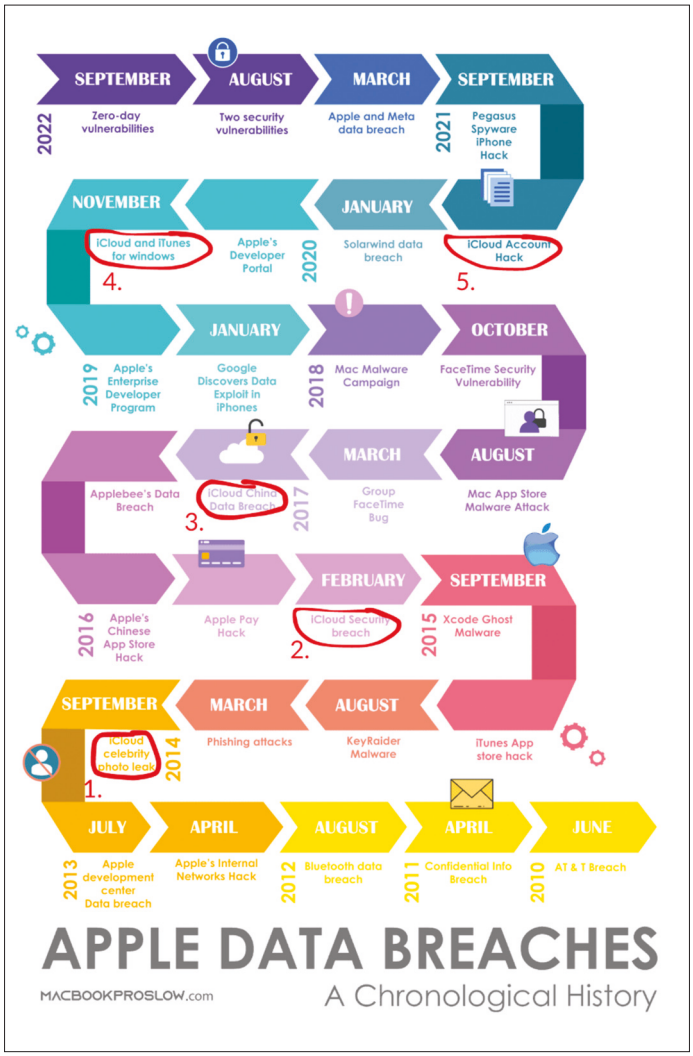


Data en tijden dat de computer unlocked was, zoals te zien in de logging.

Of voor de snelle gebruiker: (command) + (spatie), dit opent een zoekvenster. Typ dan in 'terminal' en dan ben je er ook.

iCloud

iCloud speelt een cruciale rol in het Apple-ecosysteem en biedt gebruikers verschillende voordelen. Het stelt je in staat om naadloos gegevens te synchroniseren en te delen tussen al jouw Apple-apparaten, waaronder: iPhones, iPads, Macs en zelfs Apple Watches. Hierdoor krijg je altijd en overal toegang tot de voor jou belangrijke informatie en beheer je jouw digitale leven efficiënter. Hoewel iCloud een waardevolle dienst is, zijn er in het verleden enkele



In deze afbeelding van Devansh Kamdar zie je 5x wat grootschalig fout is gegaan met iCloud

incidenten geweest die de beveiliging in twijfel hebben getrokken.

Neem de Celebrity Photo Leak: in 2014 vond er een inbreuk op de iCloud-beveiliging plaats, waarbij de privéfoto's van verschillende beroemdheden werden gestolen en online verspreid. Dit incident benadrukte het belang van sterke wachtwoorden, tweestapverificatie en het vereiste gebruikersbewustzijn bij het beveiligen van iCloud-accounts.

In een afbeelding van Devansh Kamdar zie je 5x wat grootschalig fout is gegaan met iCloud. En omdat iCloud verbonden is met al jouw apparaten, waar al jouw documenten in opgeslagen staan alsook dat er kritische services aan verbonden zijn (zoals ApplePay) is iCloud een gezocht doelwit van criminelen, waar je op zich weinig aan kan doen, behalve 2FA aanzetten en ervoor zorgen **dat je de best mogelijke beveiliging hebt geregeld**.

Linux

Zoals al eerder in dit artikel is genoemd: Mac-OS is gebaseerd op UNIX. Tal van Linux-principes rond beveiliging en het beheren van het OS-systeem zie je daarom terug bij Mac-OS. Dat is een mooie aanzet voor ons volgende artikel over Linux-systemen. Ondanks dat Linux-systemen weinig ingezet worden voor laptops (behalve door programmeurs), zijn Linux-systemen wel zeker de standaard voor stabiel draaiende (applicatie) servers. En dat ondanks het feit dat veel organisaties ervaren Linux-beheerders missen om deze servers goed te beveiligen.
Heb je van tevoren al vragen over Linux-systemen? Of onderwerpen die je graag terugziet in het artikel? Laat het vooral weten door ons een bericht te sturen of de vraag in te brengen via het LinkedIn-account van het IB Magazine.

Referenties

(1) MalwareBytes, 2020: https://go.malwarebytes.com/rs/805-USG-300/images/MWB_StateOfMalwareReport2021.pdf?aliId=eyJpIjoieW4rRGx6MFlJbDJkWEZnbiIsInQiOiJ3V1ZTSVBHSVdzdWRNVVNHRzVtVWNBPT0ifQ%253D%253D

(2) Statcounter, 2023: https://gs.statcounter.com/os-market-share/desktop/worldwide/#monthly-202001-202307-bar

(3) InformatieBeveiliging Magazine, uitgave 4 2023 https://www.macrumors.com/2021/08/24/scammer-hacks-icloud-accounts-for-nude-photos/