White paper

Device Management

– Central styring af virksomhedens data og computere

PC'er og smartphones uden for virksomhedens kontrol er den største trussel mod forretningen. Med Device Management på hardware-niveau kan virksomheden genvinde kontrollen over sine enheder – og dermed over sine data.

Siden 2002 er praktisk talt alle nye personlige computere produceret med en central funktion, der gør det muligt at kontakte og kontrollere maskinen via internettet. Funktionen er indlejret i hardware på computerens bundkort.

Funktionen, der er udviklet af canadiske Absolute, giver din virksomhed central og maksimal kontrol over alle virksomhedens computere og tablets.

NetCloud A/S

Naverland 2 - 2600 Glostrup - Telefon 88 444 24-7 - info@netcloud.dk

1. Virksomhedernes største sikkerhedstrussel er pc'er og telefoner udenfor kontrol

Hvert år mister virksomhederne værdier og data for milliarder på grund af bortkomne, stjålne eller dårligt vedligeholdte computere og smartphones.

Når vi taler datasikkerhed, så tænker de fleste på ondsindede og forklædte hackere med masker, der fra fjerne steder på jorden prøver at bryde ind i virksomhedernes computere og netværk. Men det er faktisk ikke den største trussel mod en virksomheds datasikkerhed. Den største trussel er sløseri eller kriminalitet fra organisationens egne medarbejdere.

Mennesker – ikke maskiner – er simpelthen den største sikkerhedsrisiko, når vi taler om datasikkerhed.

" Kun amatører angriber maskiner, professionelle går målrettet efter mennesker." Sådan udtrykker den legendariske sikkerhedsekspert Bruce Schneier det.

"Only amateurs attack machines, professionals target people."

Bruce Scheier

Medarbejderne har ikke nødvendigvis kriminelle hensigter, når de er årsag til tab af hardware, software og vigtigst af alt: Virksomhedens data. Det er ofte sløseri, uopmærksomhed eller sort uheld, når en medarbejder mister sin pc eller sin smartphone.

Men konsekvenserne er nærmest uoverskuelige. En undersøgelse, som Intel foretog i 2010, viser at en mistet pc i gennemsnit koster virksomheden mellem 200.000 og 300.000 kroner. I gennemsnit

Og virksomhederne mister mange computere – urimeligt mange. I 2014 antog FBI, at der blev stjålet 5,5 millioner pc'er de seneste tre år. Det er en ud af ti computere, og kun tre procent af dem blev fundet igen.

Mistede computere er årsag til mistede værdier for milliarder og atter milliarder af kroner og dollars.

Tyveri af pc'ere

According to the FBI, losses due to laptop theft totaled more than $3.5 million in 2005. The Computer Security Institute/FBI Computer Crime & Security Survey found the average theft of a laptop to cost a company $31,975.

In a study surveying 329 private and public organizations published by Intel in 2010, 7.1% of employee laptops were lost or stolen before the end of their usefulness lifespan.

Furthermore, it was determined that the average total negative economic impact of a stolen laptop was $49,256—primarily due to compromised data, and efforts to retroactively protect organizations and people from the potential consequences of that compromised data.

The total cost of lost laptops to all organizations involved in the study was estimated at $2.1 billion. Of the $48B lost from the U.S. economy as a result of data breaches, 28% resulted from stolen laptops or other portable devices.

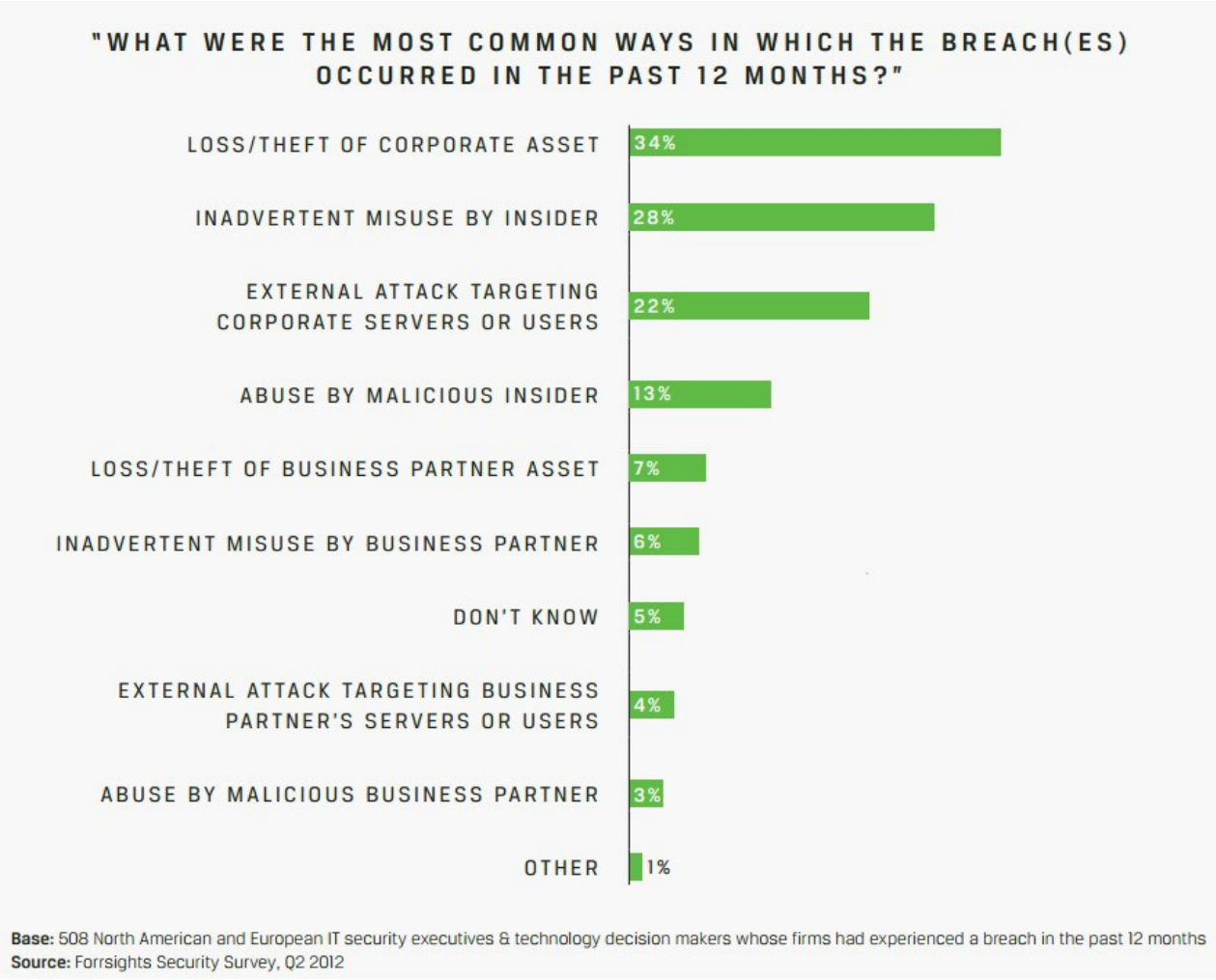
Kilde: Wikipedia.org

EU's dataforordning sætter sagen på spidsen

Den 25. maj 2018 træder EU's dataforordning i kraft. De nye regler betyder, at virksomhederne og især virksomhedernes medarbejdere i højere grad end nogensinde før bliver stillet til ansvar for virksomhedens omgang med følsomme og personlige oplysninger. Samtidig bliver bøderne for tab af data mangedoblet – helt op til fire procent af virksomhedens globale omsætning.

GDPR, General Data Protection Regulation, som den nye dataforordning hedder i daglig tale, er for alvor blevet en opgave for alle – og en afgørende forretningsparameter. Det betyder også, at alle med medarbejdere får et fælles ansvar for at beskytte virksomhedens data.

GDPR er både en trussel og en positiv drivkraft. Mange virksomheder har valgt at bruge den nye persondatalov som et signal om, at de er forrest i bussen: At de har styr på datasikkerheden. God beskyttelse af data bliver en ny konkurrenceparameter.



2. Device Management på hardware-niveau minimerer omkostninger til hardware og software og reducerer sikkerhedsrisikoen

Historisk set har pc'er været en urimeligt stor sikkerhedstrussel mod datasikkerheden. Det har simpelthen været håbløst og uoverskueligt at håndtere sikkerheden på løse laptops. Men sådan behøver det ikke være.

Microsofts Windows-styresystem og den Personlige Computer, pc, skabte i begyndelsen af 1980'erne et folkeligt gennembrud for computere. Tidligere havde computerfirmaerne haft fuldstændig magt over både hardware og software, men adskillelsen af hardware og software gav grobund for en eksplosionsagtig udvikling af programmer til IBMs pc.

Det åbne miljø, hvor tusinder og atter tusinder af tredjepartsleverandører kunne byde ind med software, gav også store problemer med at styre, hvem der havde adgang til maskiner og data. Havde man uretmæssigt fået adgang til en maskine, kunne kriminelle igen og igen forsøge at bryde kryptering og andre sikkerhedssystemer – eller ganske simpelt slette det hele og installere ny software på den stjålne hardware.

I de efterfølgende årtier blev pc'er en central del af alle virksomheders forretning – sammen med internettets udbredelse. Alle medarbejdere fik en bærbar pc som værktøj til at løse deres arbejdsopgaver.

Men det var (og er) et grundlæggende problem at styre de mange millioner af mobile computere. Hardwaren er i sig selv værdifuld, softwaren ligeså, men allerdyrest er virksomhedens risiko for at miste sine egne data, hver gang en medarbejder glemmer, taber eller får stjålet en pc.

6 karakteristika ved Device Management på hardware-niveau

1. Fjernkontrol over en enhed uanset installeret operativsystem – også hvis der ikke er installeret operativsystem.
2. Adgang til at låse enheden eller slette indhold på den.
3. Lokationsbestemme enhed.
4. Sikre at virksomhedens kritiske applikationer som antivirus, Bitlocker eller SCCM-agent altid er installeret.
5. Fjernstyre installation af tredjeparts-applikationer, lægge patches og opdateringer ud på alle enheder.
6. Samlet overblik over virksomhedens hardware og software. Hvor det befinder sig, hvordan det bliver brugt, hvilken tilstand det befinder sig i – og om er fjernet hardware eller systemer.

Patenter, forretningshemmeligheder, kundedatabaser, strategier, personlige og følsomme oplysninger kan være uvurderlige for forretningen – og i praksis ligge i enhver medarbejders plasticpose, når han eller hun tager toget hjem fra arbejde.

Gennem tiden har mange forsøgt at udvikle og implementere softwarebaserede løsninger til at kryptere, spore, låse, styre og måske slette mistede pc'er. Men mange af systemerne er kommet til kort i mødet med virkeligheden: Software kan kompromitteres, ændres eller slettes.

I 2002 havde den canadiske virksomhed, Absolute, held med at overtale IBM til at lægge en ekstra funktion ind på bundkortet til pc'er. En hardware-baseret funktion, Device Management, der kan styre pc'en via internettet. I dag har langt de fleste personlige computere uanset processor og leverandør denne funktion bygget ind i en særskilt ROM (Read Only Memory) på bundkortet.

Absolute har patent på ROM-enheden og den tilhørende software.

Da Absolutes ROM-enhed i sin tid blev installeret på bundkortet, var de fleste computere stadig desktop-maskiner bundet til en fast lokation og i nogle tilfælde endda uden internetforbindelse. I dag er de fleste computere altid på farten, i brug på kontoret, hjemmefra, i lufthavne, fly eller tog, mødelokaler i virksomheden eller hos samarbejdspartnere.
Til gengæld er pc'er i praksis altid forbundet til internettet, så ROM-enheden har i dag endnu større berettigelse og funktion. Med Absolutes ROM-enhed aktiveret kan virksomheden kontrollere, opdatere, låse og slette sine eksterne enheder, uanset hvor de befinder sig.

Device Management har fat i roden af en pc

Absolutes firmware ligger som en særskilt ROM-enhed på bundkortet fra leverandøren. Det betyder, at dens funktion er uafhængig af operativsystemet. Ved at bygge Device Management ind i selve hardwaren, udviklede Absolute i virkeligheden en lille genistreg, der genskabte kontrollen over computeren.

Absolutes ROM-enhed til Device Management er som udgangspunkt ikke aktiveret på en ny pc. Det er en optional funktion, der valgfrit kan aktiveres. ROM-enheden kan aktiveres direkte fra producenten efter aftale – typisk ved større leverancer af pc'ere. Den kan også aktiveres individuelt på et senere tidspunkt.

Device Management skaber en hardwarebaseret "tunnel" fra enhver pc med Device Management til en central styrepult, en konsol. Det betyder, at funktionen er aktiv, krypteret og sikker uanset hvilket operativsystem og hvilken version af operativsystemet, der ligger på maskinen – og helt udenom de programmer (applikationer), der i øvrigt er installeret på computeren.

Device Management har bogstavelig fat om roden af en pc via ROM-enheden på bundkortet. Hvis en pc er mistet eller stjålet, giver Device Management magten tilbage til ejeren af pc'en.

Alle systemer kan overvåges – næsten

Absolutes ROM-enhed er fabriksmonteret på alle pc-fabrikater undtaget enkelte modeller fra Sony.

MacOS-enheder, Chromebooks, smartphones og tablets med Android-styresystemet kan også administreres via løsningen.

Enheden er ikke installeret på iPhones og iPad, der har sine egne sporings- og sikkerhedssystemer.

Sådan fungerer det

1. step – hardware
Teknologien er et tæt ægteskab mellem hardware og software. Første skridt er hardware-baseret og installeret, når computeren bliver produceret på fabrikken. ROM-enheden er bygget ind i desktop- og bærbare computere, tablets og smartphones – klar til at blive aktiveret.

2. set – software
Når software-agenten er installeret, bliver ROM-enheden aktiveret og der bliver skabt kontakt mellem enheden og virksomhedens centrale konsol, der herefter overvåger og kontrollerer enheden.

3. step – persistence
ROM-enheden kontrollerer konstant, om software-agenten er installeret på computeren. Er den fjernet (uforsætligt eller med vilje), vil ROM-enheden geninstallere agenten. Selv hvis ROM-enheden bliver flashet, harddisken blanket ud eller udskiftet eller tablet-computeren eller smartphonen bliver nulstillet til fabriksindstillinger, vil ROM-enheden geninstallere software-agenten og tjekke flere hundrede sikkerhedsindstillinger på enheden. Samtidig vil systemet genskabe forbindelsen til konsol, så virksomheden kan genvinde kontrollen over enheden.

3. Central kontrol af alle elektroniske enheder

Gennemgang af konsollens funktioner og muligheder

Den centrale funktion i Absolutes sikring af virksomhedens perifere enheder er en konsol, der løbende er i kontakt med hver enkelt enhed

Man kan sige, at konsollens mange funktioner til overvågning og kontrol af enheder gør virksomhedens IT-sikkerhedspolitik operationel.

Konsollen kan blandt andet:

- Slette alt på en pc. Slette-funktionen kan overskrive harddisken op til syv gange. Det svarer til wiper-kravene i mere end 100 lande. Rapport om sletning sendes til konsol.
- Låse pc'en med en meddelelse på skærmen.
- Hente data hjem fra enheden, når den får internetforbindelse.
- Spore enheden overalt i verden (lokationsbestemmelse). Sporing kan ske via WiFi, GPS, 3G/4G-kort.
- Sikre at virksomhedens kritiske applikationer altid er installeret og opdaterede. Det kan være antivirus, SCCM-agent, Bitlocker osv.
- Give et samlet overblik over virksomhedens hardware og software.
- Scanning for data, der ikke må være på enheden. Det kan for eksempel være ulovlige persondata, oplysninger om kreditkort, fortrolige udviklingsdata mv.
- Glemte, stjålne eller mistede enheder kan rapporteres i konsollen, der varetager den vedtagne procedure mht. kontrol over enhed, eftersøgning og evt. sletning.
- Der kan opsættes alarmer via mail, sms eller oversigter (rapporter).
- Dokumentation til intern revision – op til fem år tilbage på alle enheder.
- Opsætning af virtuelt hegn med regler for, hvad der skal ske, hvis hegnet brydes.
- Integration til Microsoft System Center (SCCM), SIEM-systemer (Security Insident & Event Management), service systemer m. fl.

Harddisken sladrer

Hvis en harddisk med en Absolute agent fjernes fra pc'en og installeres på en anden pc, så vil agenten aktivere ROM-enheden på bundkortet på den nye pc – og melde tilbage til konsollen, hvor harddisken nu befinder sig. Og give magten over harddisken til den nye pc.

Sikring af eksterne enheder

Center for Internet Security, CIS, foreslår fem enkle skridt, der kan forhindre op til 80 procent af angrebene mod virksomhedens IT-sikkerhed.

- Vedligehold en ajourført liste over autoriserede og uautoriserede enheder.
- Vedligehold en ajourført liste over autoriseret og uautoriseret software.
- Udvikl og kontroller sikker konfiguration af alle enheder.
- Foretag løbende (automatiseret) vurdering af sårbarheder og korrektion af fejl.
- Overvåg og kontroller aktivt brugen af administrative rettigheder.

4. Sikkerheden i Device Management

Den tekniske sikkerhed

Absolutes ROM-enhed kommunikerer med den centrale konsol over en krypteret https-forbindelse, der fungerer uanset, om computeren er installeret med et operativsystem eller ej. Det betyder, at kontakten til enheden og sikkerheden er intakt, selv om operativsystemet eller de tilhørende sikkerhedsapplikationer er slettet eller de-aktiveret på computeren.

En enhed kan kun være forbundet til en central styringspult (konsol) ad gangen. Det betyder, at det kun er virksomheden, der har adgang til sine enheder. Det er kun Absolute, der kan ændre, hvilken virksomhed enheden er forbundet til.

46.632 genfundne pc'ere

Siden 2002 har Absolute fundet næsten 50.000 forsvundne computere.

I Danmark er der skabt kontakt til 171 enheder. Heraf er de 103 skaffet tilbage og genetableret.

Absolutes ROM-enhed er aktiveret på mere end en milliard computere hos mere end 15.000 virksomheder.

Hvis kritiske applikationer bliver slettet fra enheden, vil ROM-enheden prøve at geninstallere dem. Man kan sige, at systemet har en automatisk selv-helende funktion.

Virksomheden kan i forvejen sætte en række sikkerhedsparametre op på sine eksterne enheder, der virker både online og offline. Det kan for eksempel være sletning eller låsning af computeren, hvis den har været offline i en given periode. Det betyder, at sikkerheden vil være intakt, når maskinen har været offline i en periode – selv om den ikke har været på nettet i den mellemliggende periode.

Når maskinen igen kommer online, vil systemet spore den.

Den forretningsmæssige sikkerhed

Absolute er en vel-etableret canadisk sikkerhedsvirksomhed med hovedkvarter i Vancouver og kontorer i en lang række lande kloden over. Absolute er certificeret med alle de toneangivende certifikater i sikkerhedsbranchen som blandt andre HITRUST, SANS Top 20, NIST 800-53, COBIT, ISO og PCI-DSS compliance standards.

Om NetCloud

NetCloud er cerficeret Absolute-samarbejdspartner i Danmark. Netcloud kan på vegne af Absolute give virksomheder absolut kontrol over deres eksterne enheder – uanset hvor i verden de befinder sig. Online eller offline.

Jeres virksomhed kan købe licenser til Absolutes konsol og adgang til alle eksterne enheder. Eller I kan vælge at lade Netcloud monitorere virksomhedens enheder 24/7 til en fast månedlig ydelse.