



Overall, altijd, via eender welk device toegang hebben tot bedrijfsdata doet ook het aantal risico's toenemen. Met elk device opent zich een nieuwe toegangspoort naar uw bedrijfsdata. Een poort die u dan best van stevige grendels voorziet. Maar dat is lang niet alles. Omdat het onderscheid tussen werk- en privégebruik steeds vager wordt, moet u er rekening mee houden dat zelfs uw beste werknemers onbewust 'slechte' dingen kunnen doen op het internet en zo bijkomende beveiligingsrisico's in het leven roepen. Realdolmen helpt u om de veiligheid van uw mobiele omgeving te verhogen.

UITDAGINGEN

- Waar voorheen zakelijke toestellen zelden de veilige bedrijfsomgeving verlieten, nemen werknemers hun toestellen vandaag mee naar plaatsen waar ze blootgesteld worden aan allerlei malware en aanvallen.
- Dropbox, E-mail, WeTransfer enz., uw werknemers gebruiken het allemaal om gegevens door te sturen. Hoofdbreken voor uw IT-afdeling die hierover geen controle heeft. En toch kan het blokkeren van deze diensten nefast zijn voor de bedrijfsvoering.
- Security is geen deeltijdse job. Security wordt steeds complexer en de hoeveelheid gegevens om te analyseren is zo groot dat het voor het gemiddelde bedrijf vandaag niet haalbaar meer is hier zelf volledig voor in te staan.

EEN GREEP UIT ONZE OPLOSSINGEN:

EEN "ALWAYS ON" WERKPLEK

Gezien de onafhankelijkheid van plaats, tijd en device vereist de moderne digitale werkplek een specifieke security-aanpak die opgewassen is tegen allerlei aanvallen, intelligente malware, cyberincidenten en hackers. Realdolmen voorziet hiervoor oplossingen gebaseerd op een geïntegreerd hybride securitymodel. Automatische bijsturing en proactief optreden staan hierbij centraal.

Symantec | CheckPoint | Fortinet | WatchGuard | Microsoft
Advanced Threat Analytics

BEVEILIGEN VAN KRITIEKE EN PRIVACYGEVOELIGE DATA

IT draait steeds meer om het 'enablen' van de business en businessinnovatie dan wel om controle. Bedrijven zijn meer 'open' door zowel menselijke samenwerkingsverbanden als digitale koppelingen. Het model waarbij het bedrijf beveiligd is als een fort met slechts één in- en uitgang is vandaag niet meer van toepassing en wordt als verouderd beschouwd. Een firewall alleen als beveiliging volstaat niet meer.

Vandaag is het belangrijk om uw belangrijkste bedrijfsprocessen, -applicaties en data te beschermen als de 'kroonjuwelen' van het bedrijf. Hiervoor worden mitigatietechnieken gebruikt zoals dataclassificatie, digital rights management, data loss prevention en encryptie. Realdolmen voorziet een holistische oplossing op maat van uw bedrijf.

Azure Rights Management | Varonis



SECURITY AWARENESS

Een hacker gaat altijd op zoek naar de zwakste schakel in het systeem. Meestal is dat de mens. Mensen blijven maar klikken op links en buttons zonder zich veel vragen te stellen. Bovendien gaan criminelen steeds professioneler te werk waardoor het voor de eindgebruiker moeilijker wordt om de legitimiteit van een website of e-mail vast te stellen. Aanvallen worden soms ook, en steeds vaker, specifiek gericht op een bepaald persoon. Daarbij wordt alles uit de kast gehaald om de eindgebruiker om de tuin te leiden. De aandacht voor digitale veiligheid bij eindgebruikers verhogen, is in veel gevallen de beste actie om de algemene beveiliging te verhogen. Realdolmen wil naast de bewustwording ook een gedragswijzing bij de eindgebruikers teweeg brengen, een meerwaarde in elke GDPR compliency roadmap.

Kaspersky | CheckPoint | Realdolmen Education

RELEVANTIE EN EFFECTIVITEIT VAN SECURITY VIA SOC-AS-A-SERVICE

Traditionele beveiligingstools implementeren en onderhouden, is altijd al een moeilijke en budgetgevoelige oefening geweest voor elke doorsnee organisatie. Niet verwonderlijk dan ook dat enerzijds oplossingen implementeren die opgewassen zijn tegen cyber threats, anderzijds de mankracht en expertise om deze oplossing 24x7 te monitoren en te optimaliseren een onhaalbare kaart lijkt te zijn. De TCO om dit te realiseren is immers hoger dan elk voorgaand security-traject. Althans zonder security-incident....

Realdolmen biedt voor deze problematiek een 24x7 SOC-as-a-serviceoplossing aan (SOC: Security Operation Center). Geen zware CAPEX gecombineerd met de eindeloze zoektocht naar betaalbare competentie, maar een ontzorgend OPEX-model met snelle adoptie gebaseerd op best-of-breed technologie en expertise. Een mogelijk alternatief voor een jarenlang uitgesteld SIEM-traject (Security information and event management)? Een realistische strategie voor datalekpreventie en -detectie, conform de GDPR-wetgeving? Realdolmen vertelt u er graag meer over.

SecureWorks

'Secure Business Enablement' is onderdeel van Realdolmens Engaged Workplace offering

"Engaged Workplace" betekent voor Realdolmen:

- Gemotiveerde medewerkers
- Gedigitaliseerde bedrijfsprocessen
- Een geoptimaliseerd HR-beleid
- Een flexibele en beveiligde IT-infrastructuur
- Werken mogelijk maken vanop eender welke locatie, op eender welk tijdstip op eender welk device
- Slimmer samenwerken en communiceren
- Medewerkers opleiden om de nieuwe werkplek efficiënt te gebruiken
- Een cultuur opbouwen die de nieuwe werkplek omarmt