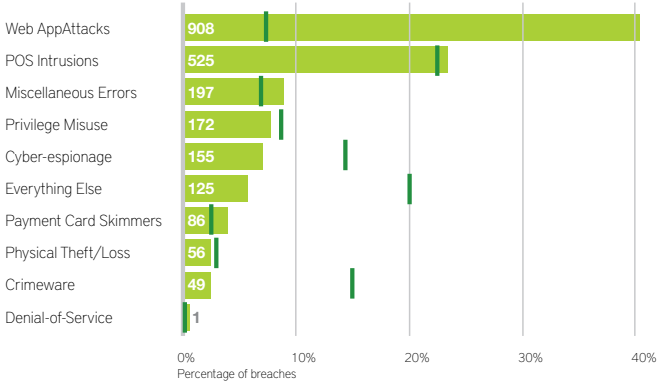
REALDOLMEN
to get there, together

HYBRID CLOUD
IDENTITEITSBEVEILIGING

Hybrid Cloud Identiteitsbeveiliging

Verizon publiceert jaarlijks zijn Data Breach Investigations Report (DBIR). Elk jaar opnieuw sturen organisaties hun data over duizenden beveiligingsincidenten en data-inbreuken naar Verizon. Onderzoekers analyseren deze informatie om nieuwe patronen, blijvende trends en interessante nieuwtjes te identificeren in het veranderende digitale bedreigingslandschap.

PERCENTAGE, AND COUNT OF BREACHES PER PATTERN.



TOP THREAT ACTION VARIETIES WITHIN INCIDENTS INVOLVING CREDENTIALS

source: http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

HET DBIR 2016 VERMELDT:

- incidenten in meer dan 82 landen
- in de overheids-, entertainment-, financiële en informatiesectoren
- meer beveiligingsincidenten dan data-inbreuken
- bevestigde openbaarmaking (niet gewoon potentiële openbaarmaking) van data aan een onbevoegde partij
- 1.429 incidenten van identiteitsdiefstal

Jammer genoeg worden vaak niet genoeg inspanningen geleverd om mogelijke veiligheidsbedreigingen in te perken. Veiligheid zou voor iedereen in elk bedrijf een bekommernis moeten zijn, van C-niveau tot System Engineer. Toch blijken veiligheidsmaatregelen die enkele jaren geleden nog 'in' waren, niet langer van toepassing. Een nieuwe benadering is nodig zodat onze bedrijfsdata onze bedrijfsdata blijven, en niet die van iemand anders.

VRAGEN DIE U ZICH BEST STELT

Dit zijn enkele van de vele vragen die u zich moet stellen met uw eigen omgeving in gedachte:

HEBT U VEEL GEPRIVILIGEERDE ACCOUNTS ZOALS DOMAIN ADMINS?

Door onnodige rechten toe te kennen aan gebruikers kunnen ze buiten hun toegelaten werkgebied handelen. We willen gebruikers enkel de toegangsrechten geven die ze effectief nodig hebben om hun dagelijkse taken uit te voeren.

KUNT U ACTIES TRACEREN NAAR DE PERSOON DIE ZE HEEFT UITGEVOERD, HET UUR VAN UITVOERING EN HET BRONSYSTEEM?

Auditing moet steeds een integraal deel zijn van een IT-organisatie zodat duidelijk kan worden bepaald wat er mis is gegaan, door wie, wanneer en waar.

WORDEN UW WEBAPPLICATIES VEILIG GEPUBLICEERD VOOR DE BUITENWERELD?
Applicaties toegankelijk maken voor gebruikers buiten het netwerk is één ding, ervoor zorgen dat dit veilig gebeurt, een heel ander.

PAST U USER LIFECYCLE MANAGEMENT TOE VOOR GEBRUIKERS DIE DE ORGANISATIE VERLATEN OF GEBRUIKERS DIE BINNEN HET BEDRIJF EEN ANDERE ROL KRIJGEN?
Een inactieve gebruikersaccount bijvoorbeeld kan worden gebruikt om toegang te krijgen tot bepaalde data en dit zonder op te vallen aangezien het een geldige account is.

WORDEN APPLICATIES ENKEL DOOR WACHTWOORDEN BEVEILIGD?
Multifactor-authenticatie helpt de toegang tot data en applicaties beschermen. Voor eindgebruikers betekent dit wel dat ze een extra stap moeten uitvoeren, maar dit kan naadloos en toch met een extra beveiligingslaag gebeuren.

BENT U BESCHERMD TEGEN PASS-THE-HASH-AANVALLEN? HEBT U BINNEN UW ORGANISATIE EEN DEGELIJK WACHTWOORDBELEID?
Zonder een goed wachtwoordbeleid kunt u zich niet beschermen tegen tal van verschillende aanvallen. Toegang tot één machine kan toegang betekenen tot meerdere machines

CONTROLEERT U HET INLOGGEDRAG IN UW ORGANISATIE? WAAR LOGGEN MENSEN IN? HOEVEEL POGINGEN DOEN ZE?
Het overgrote deel van de beveiligingsinbreuken vindt plaats wanneer aanvallers zich toegang verschaffen tot een omgeving door de identiteit van een gebruiker te stelen. Met enkele specifieke tools en met de hulp van Machine Learning kunt u inloggedrag controleren en analyseren.

WAT BIEDEN WIJ?

Realdolmen is uw gids naar een veiligere hybride identiteit. Samen bepalen we hoe we uw huidige omgeving het niveau van identiteitsbeveiliging kunnen geven dat aan de huidige tijd is aangepast.

Gedurende 4 tot 8 dagen evalueren we uw risico's en zwakke punten. We identificeren aanbevelingen en bepalen de aanpak voor een veilige hybride identiteit.

De conclusies van deze evaluatie worden in een presentatie van een halve dag voorgesteld evenals in een verslag met aanbevelingen, best practices uit de sector en projectdefinities.

Naast deze eerste evaluatie biedt Realdolmen een jaarlijkse opvolging aan om de gemaakte voortgang te identificeren aangezien veiligheid niet statisch is maar continu evolueert.

VOORDELEN VAN EEN BEVEILIGDE HYBRIDE IDENTITEIT

- Zonder zorgen applicaties publiceren voor de buitenwereld.
- Eindgebruikers meer vertrouwen geven in IT-systemen en -beheerders.
- Geen paniek meer bij een externe audit.
- Niet langer enorm veel tijd besteden aan het opsporen van kwaadaardige aanvallen in uw organisatie.
- Een tevreden Chief Security Officer.

GEÏNTERESSEERD?

Bent u bereid om het aanvaloppervlak van uw bedrijf te verkleinen? Wilt u niet in het data-inbreukrapport van Verizon belanden? Wilt u dat wij uw gids zijn naar een veiligere identiteitsinfrastructuur?

Neem voor meer informatie contact op via :
info@realdolmen.com

V.U.: NV RealDolmen SA, A. Vaucampslaan 42, B-1654 Huizingen.

REALDOLMEN
info@realdolmen.com
WWW.REALDOLMEN.COM
A. Vaucampslaan 42
B-1654 Huizingen
TEL +32 2 801 55 55