Bijlage 5 – Eisen voor het hosten van externe gegevens

Deze vereisten zijn van toepassing op het hosten van alle applicaties en gegevens van BT die 'Vertrouwelijk' (IC) of Strikt Vertrouwelijk' (ISC) zijn, op elke locatie die niet in eigendom van BT is of niet door haar wordt beheerd. Dit omvat maar is niet beperkt tot Cloud-diensten waar a) de gegevens in transit veilig en beschermd worden tegen onderschepping, meestal met behulp van een gecodeerd protocol, en b) de BT-gegevens in rust worden gecodeerd binnen de cloud-dienst.

Voor het hosten van Vertrouwelijke applicaties en gegevens buiten BT gelden de volgende voorwaarden:

- Het datacenter moet beschikken over een geldige ISO 27001 certificering (of certificering (en)) waarmee wordt aangetoond dat er gelijkwaardige controles worden uitgevoerd voor veiligheidsbeheer, of zal voldoen aan de Veiligheidsvereisten volgens de ISO 27001 certificering of het veiligheidsbeleid in overeenstemming met ISO27001 en/of toewerken naar ISO27001 binnen een termijn overeengekomen met BT;
- Gegevens 'in transit' moeten sterk worden gecodeerd ter bescherming van de gegevens van BT tussen het punt waar zij BT uitgaan, en de DC-grens (meestal de load balancer en decoderingsinrichting gelegen achter de firewall van de DC-grens);
- DC-ingenieurs met fysieke toegang tot de servers dienen geen logische toegang hebben tot de productie-omgeving, en beheerders met logische toegang tot de systemen moeten geen fysieke toegang hebben tot de DC.
- Alle logische toegang moet worden gecontroleerd door het beveiligingssysteem om te zorgen dat het beheer van wachtwoorden gecontroleerd verloopt en dat het juiste proces van toegangsrechten wordt gebruikt om de aanvrager te identificeren, bijv. CyberArk.
- Voor bevoorrechte toegang (inclusief maar niet beperkt tot DBA) moet het beheer van wachtwoorden aan tijd gebonden zijn en waar mogelijk worden er extra beperkingen ingevoerd op het IP-bron adres.
- Een bevoorrechte toegang tot bijvoorbeeld DBA, ASG, enz. naar systemen die BT-informatie verwerken, moet voldoen aan de eisen in bijlage 1 - classificatie van informatie.- .
- Voor toegang op afstand moet een veilig Virtueel Private Network worden gebruikt in combinatie met de op functie baseerde verificatie met twee factoren; daarnaast kan elke externe derde partij met bevoorrechte toegang alleen toegang krijgen tot de systemen waar BT-gegevens in transit zijn of in rust, binnen hetzelfde land als de DC, of een land of gebied dat zorgt voor een passend beschermingsniveau voor de BT-gegevens;
- Implementeren van hele leven cryptografische sleutelbeheer-processen volgens de beste praktijken uit de sector;
- Elke fysieke toegang tot domeinen of apparatuur waar BT- informatie is opgeslagen of wordt verwerkt, moet een controleerbaar proces doorlopen bijv. door het wijzigen van een verzoek, zodat toegang alleen wordt verleend voor de minimale duur die vereist wordt, en er bijvoorbeeld geen permanente toegang wordt verschaft;
- De opslag van back-upgegevens buiten de locatie moet worden gecodeerd in overeenstemming met de voorschriften van bijlage 1;
- Controles moeten onbevoegde toegang verminderen, detecteren en voorkomen. Controles moeten een audit-traject creëren met behulp van het "wie wat waar wanneer" principe.
- Wie de gebruiker was, bijvoorbeeld gebruikersaccount-ID;
- Tot welke activa ze toegang hadden, bijvoorbeeld gegevens;
- Van waar ze toegang tot het goed hebben gekregen, bijvoorbeeld IP-adres; en
- Wanneer, bijvoorbeeld tijdstempel.

- Alle fysieke en logische toegang moet worden aangemeld, met logbestanden die 1 jaar worden bewaard (minimaal);
- In het geval van een overtreding waarbij BT-gegevens wordt gecompromitteerd, gestolen of gewijzigd, moet een proces worden ingesteld om ervoor te zorgen dat BT binnen een redelijke tijdsperiode over voldoende informatie beschikt;

Waar er ISC-informatie is, geldt bovendien het volgende -

- het het datacenter moet een on-site veiligheidsinspectie doorlopen;
- Applicatieservers, gegevensbestanden, enz., moeten op speciale, niet multi-beheerde, infrastructuur worden gebruikt en hosting moet plaatsvinden binnen een specifiek rek in een veilige kooi. Indien niet aan dit voorschrift niet kan worden voldaan, moet d.m.v. een risico-evaluatie van BT gegarandeerd worden dat er een adequate scheiding bestaat tussen BT-gegevens en de gegevens van andere klanten die dezelfde omgeving delen, en worden gezorgd dat DBA's geen log-in toegang hebben tot processen van klanten, en deze ook niet op een verzamelde manier zien. Databasetabellen en rijen moeten niet een overzichtsweergave zijn van het proces van één klant.
- Er moeten processen worden ingesteld om ervoor te zorgen dat de ISC-gegevens veilig worden verwijderd aan het einde van de levenscyclus in de cloud; Alle opslagapparaten met ISC-gegevens moeten worden gewist of verwijderd zoals gespecificeerd in bijlage 1;