Overzicht van de technische en organisatorische beveiligingsmaatregelen bij Proximus

1. Organisatie van de beveiliging bij Proximus

Het **departement Security Governance and Investigation,** onder leiding van **Group Corporate Affairs,** is verantwoordelijk voor de aspecten Security Governance, Security Management en Cyber Security Monitoring and Response van de organisatie.

Security Governance is verantwoordelijk voor het informatiebeveiligingskader van Proximus, waaronder de definitie en het beheer van de policy's inzake informatiebeveiliging en van de beveiligingsarchitectuur.

Security Management evalueert of bedrijfsprojecten voldoen aan de beveiligingspolicy's, doet risicoanalyses inzake informatiebeveiliging voor projecten, staat in voor activiteiten in het domein van kwetsbaarheidsbeheer en pentestbeheer en meet en rapporteert over de conformiteit met policy's inzake informatiebeveiliging.

Onder **Cyber Security Intelligence & Incident Response** vallen twee teams:

- Cyber Defense Center - Het Cyber Defense Center is het centrale monitoringteam voor cybersecurityincidenten op de infrastructuur en diensten van de Proximus Groep. Het Cyber Defense Center is de klok rond actief en gebruikt de totaliteit van het Cyber Defense Center om aanvallen en intrusies zo snel mogelijk te detecteren en in te dijken.
- Proximus CSIRT - Het CSIRT van Proximus verstrekt informatie en bijstand om de risico's van cybersecurityincidenten te beperken en efficiënt op dergelijke incidenten te reageren wanneer ze zich voordoen. Het streeft ernaar om een internationaal voorbeeld te zijn voor informatie en expertise op het vlak van cyberveiligheid in alle domeinen van Incident Response. Het CSIRT van Proximus verzamelt, filtert, analyseert en verspreidt informatie over bedreigingen om proactief te kunnen communiceren over aanvallen waarvan de Proximus Groep het slachtoffer dreigt te worden.

Voor elk van de kerndivisies van Proximus werd een Security Officer als contactpersoon aangeduid om binnen Security Governance and Investigation direct te coördineren en ervoor te zorgen dat zijn divisie voldoet aan het gevestigde beveiligingskader.

2. Veiligheidsbeleidskader van Proximus

Proximus handhaaft een veiligheidsbeleidskader dat voorziet in uitgebreide controles en betrekking heeft op bestaande en opkomende onderwerpen in verband met informatiebeveiliging, die de organisatie in staat stellen om te reageren op de snelle manier waarop bedreigingen, de technologie en risico's evolueren. Het gevestigde veiligheidsbeleidskader van Proximus beoogt informatierisico's verbonden aan zijn diensten op een aanvaardbaar niveau te houden, door te reageren op snel evoluerende risico's, waaronder gesofisticeerde cybersecurityaanvallen, en door te allen tijde de toepasselijke reglementering na te leven.

Het veiligheidsbeleidskader van Proximus is trouw aan de best practices van de ISF Standard of Good Practice for Information Security, die alle onderwerpen behandelt die worden uiteengezet in ISO/IEC 27002:2013, COBIT 5 for Information Security, NIST Cybersecurity Framework, CIS Top 20 Critical Security Controls for Effective Cyber Defence and Payment Card Industry Data Security Standard (PCI DSS), waardoor het de permanente verbetering van de informatiebeveiliging binnen de organisatie bevordert en het de organisatie helpt om zich voor te bereiden op en het hoofd te bieden aan ernstige incidenten die een aanzienlijke impact kunnen hebben op de activiteiten van Proximus.

Het veiligheidsbeleidskader van Proximus sluit aan bij de structuur en de flow van de ISO/IEC 27000 'suite' van normen en ondersteunt tal van ISO 27001-certificatieprogramma's binnen de organisatie via de invoering van een systeem voor het beheer van informatiebeveiliging (Information Security Management System - ISMS).

Het veiligheidsbeleidskader van Proximus heeft onder meer betrekking op onderwerpen in de volgende domeinen:
human resources, assetmanagement, toegangscontrole, dataversleuteling, fysieke en milieuveiligheid, beveiliging van de operaties, beveiliging van de communicatie, systeemontwikkeling en -onderhoud, relaties met leveranciers, beheer van incidenten inzake informatiebeveiliging, beheer van de bedrijfscontinuïteit, conformiteit.

3. Beheer van beveiligingsrisico's bij Proximus

Het proces voor de beoordeling van beveiligingsrisico's is een kernelement voor de handhaving van de beveiliging en data privacy bij Proximus.

Het proces waarborgt voor alle projecten en systemen de uitvoering van beveiligingscontroles van Proximus en een goedkeuring door beveiligingsexperts vóór ze in gebruik worden genomen.

De methodologie voor risicobeoordeling van Proximus is afgestemd op de IRAM2-methodologie van ISF. IRAM2 is de standaardbedrijfsmethodologie die wordt gebruikt voor alle informatiebeveiligingsprojecten bij Proximus en de bij Proximus toegepaste beheerssystemen voor informatiebeveiliging gebaseerd op ISO27001. IRAM2 zijn afgestemd op de ISF Standard of Good Practice for Information Security.

4. Human resources

Het doel van beveiligingscontroles in het domein van human resources is:

- te zorgen dat werknemers en aannemers hun verantwoordelijkheden begrijpen en geschikt zijn voor de rollen waarvoor ze in aanmerking komen;
- te zorgen dat werknemers en aannemers zich bewust zijn van hun verplichtingen inzake informatiebeveiliging en ze nakomen;
- de belangen van de organisatie te beschermen in het kader van wijziging of beëindiging van de tewerkstelling.

5. Assetmanagement

Proximus gebruikt assetmanagement en dataclassificatie om traceerbaarheid en auditeerbaarheid te garanderen.

Het doel van beveiligingscontroles in het domein van assetmanagement is:

- de assets van de organisatie te identificeren en de gepaste beschermingsverantwoordelijkheden te definiëren;
- ervoor te zorgen dat informatie een gepast beschermingsniveau geniet in overeenstemming met het belang ervan voor de organisatie;
- ongeoorloofde bekendmaking, wijziging, verwijdering of vernietiging van informatie opslagen op dragers te voorkomen.

6. Toegangscontrole

Proximus heeft methodes ingevoerd om de toegang tot bedrijfsapplicaties, systemen, informaticatoestellen en netwerken te beperken door van gebruikers te eisen dat ze gemachtigd zijn vóór ze toegangsprivileges krijgen, dat ze geauthenticeerd worden door middel van toegangscontrolemechanismen en onderworpen worden aan een strikt sign-onproces vóór ze toegang krijgen.

Proximus beschikt over specifieke platformen voor identiteits- en toegangsbeheer voor zijn klanten, partners en medewerkers om functiesplitsing te garanderen, en ook over een specifieke infrastructuur voor het beheer van geprivilegieerde toegang.

Het doel van beveiligingscontroles in het domein van toegangscontrole is:

- toegang tot informatie en informatieverwerkingsfaciliteiten te beperken;
- toegang voor gemachtigde gebruikers te verzekeren en onbevoegde toegang tot systemen en diensten te voorkomen;
- gebruikers verantwoordelijk te maken voor de beveiliging van hun authenticatiegegevens;
- onbevoegde toegang tot systemen en applicaties te voorkomen.

7. Encryptie

Encryptie biedt een nog hoger niveau van beveiliging en privacy van onze diensten.

Omdat de gegevens die u creëert, bewegen tussen uw toestel, de diensten van Proximus en onze datacenters, worden ze beschermd door beveiligingstechnologieën zoals HTTPS en Transport Layer Security.

Proximus versleutelt zeer vertrouwelijke en gevoelige persoonsgegevens indien nodig.

De beveiligingspolicy's van Proximus omvatten onder meer het gebruik van pseudonimisering (de vervanging van persoonlijk identifieerbaar materiaal door artificiële identificatiegegevens) en versleuteling (de codering van berichten zodat alleen wie gemachtigd is ze kan lezen).

Het doel van encyrptie is om gepast en efficiënt gebruik van versleuteling te garanderen om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen.

8. Fysieke en milieubeveiliging

Het doel van controles in het domein van fysieke en milieubeveiliging is:

- onbevoegde fysieke toegang tot, schade aan en inmenging in de informatie en informatieverwerkingsfaciliteiten van de organisatie te voorkomen;
- verlies, beschadiging, diefstal of compromittering van assets en de onderbreking van de activiteiten van de organisatie te voorkomen.

9. Beveiliging van de operaties

Het doel van controles in het domein van de beveiliging van de operaties is:

- te zorgen voor de correcte en veilige werking van informatieverwerkingsfaciliteiten;
- te zorgen dat informatie en informatieverwerkingsfaciliteiten worden beschermd tegen malware;
- bescherming te bieden tegen het verlies van gegevens;
- gebeurtenissen te registreren en bewijsmateriaal te genereren;
- de integriteit van operationele systemen te garanderen;
- benutting van technische kwetsbaarheden te voorkomen;
- de impact van auditactiviteiten op operationele systemen te minimaliseren.

Specifiek inzake de benutting van technische kwetsbaarheden heeft Proximus een proces voor kwetsbaarheidsbeheer opgesteld om de beveiligingscyclus te vervolledigen, waarbij de levenscyclus van het project (preventieve controles) en Incident Response Management (detectiecontroles) een rol spelen, dankzij de combinatie van commercieel beschikbare en interne, op maat gemaakte tools, intensieve geautomatiseerde en manuele penetratietests, processen voor kwaliteitsbewaking, Software Security Reviews en externe audits.

Het proces voor kwetsbaarheidsbeheer van Proximus identificeert en classificeert kwetsbaarheden en coördineert remediërings- en mitigatieacties voor kwetsbaarheden die kunnen worden veroorzaakt door:
(1) fouten in het design;
(2) fouten in de codering of kwaadwillige code;
(3) fouten in de configuratie;
en een impact hebben op elementen van:
(a) componenten van besturingssystemen of netwerkcomponenten;
(b) middle components (interpreters, JRE, …);
(c) daemons, applicaties, firmware, …

Wanneer kwetsbaarheden worden geïdentificeerd, wordt een correctief pad opgestart met veranderingen aan het netwerk, de installatie van security patches, de rechtzetting van configuratiefouten, de correctie van de applicatiecode of het -ontwerp. Op die manier kan Proximus bedreigingen detecteren en erop reageren om producten te beschermen tegen spam, malware, virussen en andere vormen van kwaadwillige code.

10. Beveiliging van de communicatie

Het doel van controles in het domein van de beveiliging van de communicatie is:

- te zorgen voor de bescherming van informatie op netwerken en de ondersteunende informatieverwerkingsfaciliteiten;
- de beveiliging te handhaven van informatie die wordt uitgewisseld binnen een organisatie en met eventuele externe entiteiten.

11. Systeemontwikkeling en -onderhoud

Proximus ontwerpt met beveiliging voor ogen. Onze beveiligings- en privacyexperts werken samen met ontwikkelingsteams, die de code bijwerken en ervoor zorgen dat producten beschermd worden door een sterke beveiliging.

Het doel van controles in het domein van systeemontwikkeling en -onderhoud is:

- te zorgen dat informatiebeveiliging een wezenlijk deel uitmaakt van informatiesystemen tijdens de volledige levenscyclus. Dat omvat ook de vereisten voor informatiesystemen die diensten leveren via openbare netwerken;
- te zorgen dat informatiebeveiliging wordt ontworpen en geïmplementeerd binnen de ontwikkelingslevenscyclus van informatiesystemen;
- te zorgen dat de gegevens die worden gebruikt voor tests worden beschermd.

12. Relaties met leveranciers

Het doel van controles in het domein van relaties met leveranciers is:

- te zorgen dat de assets van de organisatie die voor leveranciers toegankelijk zijn, worden beschermd;
- een overeengekomen niveau van informatiebeveiliging en dienstlevering aan te houden in overeenstemming met de overeenkomsten met de leveranciers.

Meer in detail betekent dit dat Proximus de toegang tot uw bedrijfsgegevens beperkt tot de personeelsleden van Proximus die ze nodig hebben voor hun werk, bijvoorbeeld wanneer een medewerker van de klantendienst u bijstaat bij het beheer van uw gegevens.

Sterke toegangscontroles worden opgelegd door organisatorische en technische voorzorgsmaatregelen. Wanneer we werken met derden, bijvoorbeeld leveranciers van Customer Support, om diensten van Proximus te leveren, laten we hen een beveiligingsprogramma ondertekenen, een document met de beveiligingsvereisten van Proximus. We voeren willekeurige audits uit om er zeker van te zijn dat ze een gepast beveiligings- en privacyniveau hanteren om toegang te krijgen tot uw bedrijfsgegevens.

13. Beheer van incidenten inzake informatiebeveiliging

Het doel van controles in het domein van het beheer van incidenten inzake informatiebeveiliging is te zorgen voor een consistente en efficiënte aanpak van het beheer van incidenten inzake informatiebeveiliging, met inbegrip van communicatie over beveiligingsvoorvallen en zwakke punten.

Security Monitoring and Response is een van de kerntaken van het Proximus Cyber Defense Center en het CSIRT.

Het Security Monitoring and Response-proces werd bij Proximus ingevoerd met als hoofddoel:

- advies geven bij het nemen van beslissingen in verband met veiligheidsincidenten;
- zorgen voor een proceskader voor efficiënte 24x7 veiligheidsmonitoring (Niveau 1) en een wachtdienst (Niveau 2 en hoger) binnen Proximus, met de nadruk op eerste detectie, analyse en reactie;
- advies geven met betrekking tot prioritering en escalatie van veiligheidsincidenten;
- zorgen dat Proximus en zijn klanten de volgende voordelen genieten:
- betere algemene oplossing van incidenten dankzij een consistente en snelle monitoring, analyse, identificatie en escalatie van veiligheidsincidenten;
- betere dienstverlening dankzij gedefinieerde werkinterfaces met alle teams die betrokken zijn bij de behandeling van incidenten;
- betere en consistente rapportering om de permanente verbetering van de beveiliging bij Proximus te bevorderen.

In overeenstemming met internationale beveiligingsnormen en -vereisten hanteert Proximus een beleid inzake veiligheidslogging dat alle relevante gegevens definieert die naar het SIEM-platform van Proximus moeten worden gestuurd om een nauwkeurige monitoring van beveiligingsvoorvallen uit te voeren.

14. Conformiteit

Het doel van conformiteitscontroles is:

- inbreuken op juridische, wettelijke, regelgevende of contractuele verplichtingen in verband met informatiebeveiliging en op eventuele beveiligingsvereisten te vermijden;
- te zorgen dat informatiebeveiliging wordt geïmplementeerd en toegepast in overeenstemming met de policy's en procedures van de organisatie.

* * *