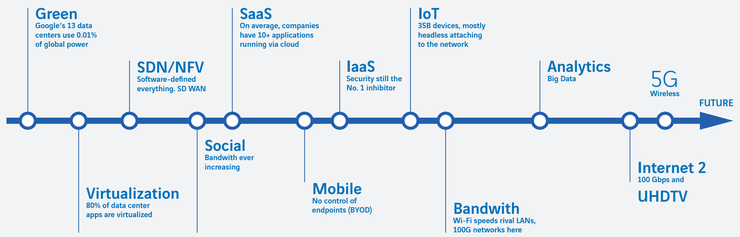
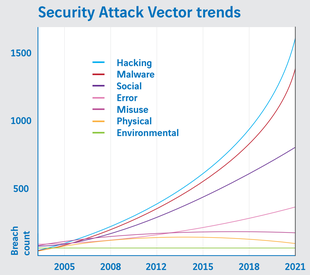
axians

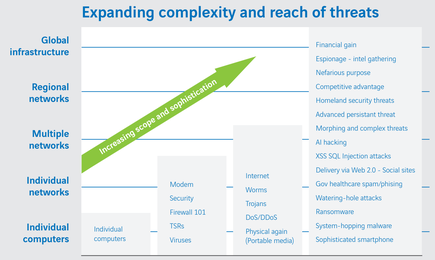
The best of ICT with a human touch

Infrastructure Change

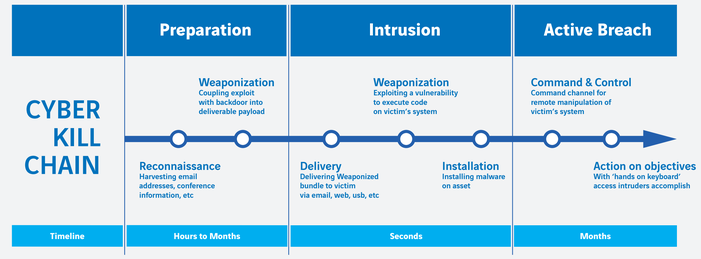


Security Trends

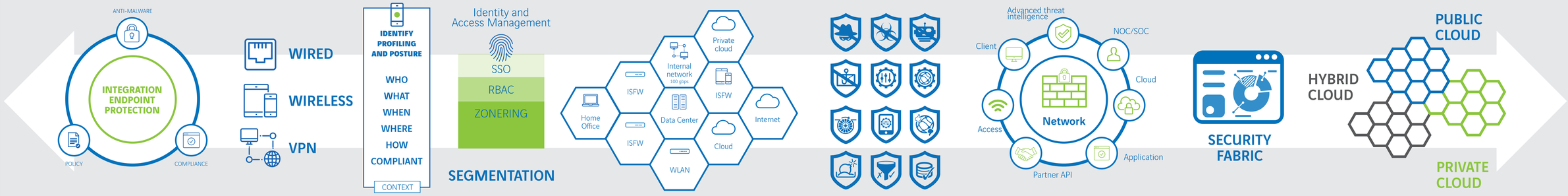




Cyber Kill Chain

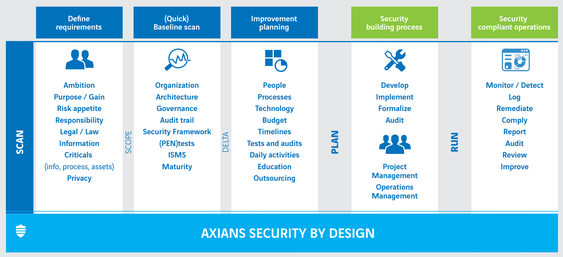


Secure Infrastructure Architecture

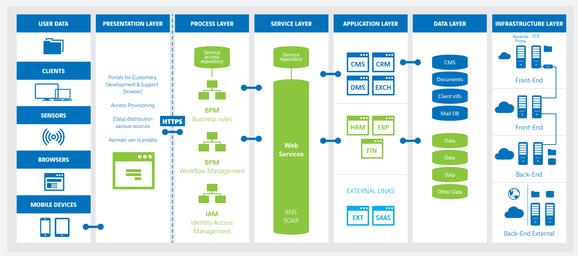


Plan-Do-Check-Act

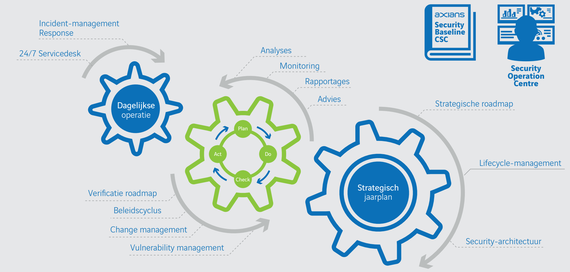
Security Planning Process



Security by Design



SOC-SIEM-Monitoring



COMPLIANCY FRAMEWORKS : ISO 27001—NEN 7510—BIG—VIR—ISA 99—PCI-GDPR-NIST—ISAE 3402

20 CIS Critical Security Controls

CSC 1
Inventarisatie van geautoriseerde en niet-geautoriseerde apparaten
Beheer actief (inventariseren, volgen en corrigeren) alle hardwareapparaten in het netwerk, zodat alleen geautoriseerde apparaten toegang wordt gegeven en niet-geautoriseerde en onbeheerde apparaten worden opgespoord en wordt voorkomen dat deze toegang krijgen.

CSC 2
Inventarisatie van geautoriseerde en niet-geautoriseerde software
Beheer actief (inventariseren, volgen en corrigeren) alle software in het netwerk, zodat er alleen geautoriseerde software wordt geïnstalleerd en kan worden uitgevoerd, en niet-geautoriseerde en onbeheerde software wordt opgespoord en wordt voorkomen dat deze worden geïnstalleerd of uitgevoerd.

CSC 3
Veilige hardware- en softwareconfiguraties op mobiele apparaten, laptops, werkstations en servers
Stel de beveiligingsconfiguratie op voor laptops, servers en werkstations, en implementeer en beheer deze configuratie actief (volgen, rapporteren en corrigeren) met een grondig configuratiebeheer- en wijzigingscontrole-proces om te voorkomen dat aanvallers kwetsbare services en instellingen misbruiken.

CSC 4
Doorlopende evaluatie en herstel van beveiligingsproblemen
Win doorlopend nieuwe informatie in, evalueer deze en onderneem er actie op om beveiligingsproblemen te identificeren en aanvallers geen of nagenoeg geen kans te geven.

CSC 5
Gecontroleerd gebruik van beheerdersbevoegdheden
Volg, controleer, voorkom en corrigeer gebruik, toewijzing en configuratie van beheerdersmachtigingen voor computers, netwerken en toepassingen.

CSC 6
Onderhoud, bewaking en analyse van auditlogboeken
Verzamel, beheer en analyseer auditlogboeken met gebeurtenissen waarmee u een aanval kunt detecteren, begrijpen of herstellen.

CSC 7
Bescherming voor e-mail en webbrowsers
Minimaliseer het aanvalsoppervlak en de kansen van aanvallers om menselijk gedrag te manipuleren door middel van hun interactie met webbrowsers en e-mailsystemen.

CSC 8
Verdediging tegen malware
Controleer de installatie, verspreiding en uitvoering van schadelijke code op meerdere punten in de onderneming en optimaliseer tegelijk het gebruik van automatisering om snel de verdediging te herzien, gegevens te verzamelen en een correctieve actie te ondernemen.

CSC 9
Beperkingen en controle van netwerkpoorten, protocollen en services
Beheer (volgen, controleren en corrigeren) het doorlopende, operationele gebruik van poorten, protocollen en services op netwerkapparaten om de kansen te minimaliseren dat beveiligingslekken door aanvallers worden misbruikt.

CSC 10
Mogelijkheid van gegevensherstel
Maak op de juiste manier met een bewezen methodologie back-ups van cruciale informatie, zodat tijdig herstel mogelijk is.

CSC 11
Beveilig configuraties voor netwerkapparaten zoals firewalls, routers en switches
Bepaal, implementeer en beheer actief (volgen, rapporteren en corrigeren) de beveiligingsconfiguratie van netwerkinfrastructuurapparaten door middel van een grondig configuratiebeheer- en wijzigingscontroleproces om te voorkomen dat aanvallers kwetsbare services en instellingen misbruiken.

CSC 12
Verdediging aan de grenzen
Detecteer, voorkom en corrigeer de informatiestroom tussen netwerken met verschillende vertrouwensniveaus, met de nadruk op gegevens die de beveiliging aantasten.

CSC 13
Bescherming van gegevens
Voorkom gegevensdiefstal, verklein de gevolgen van gestolen gegevens en waarborg de privacy en integriteit van gevoelige informatie.

CSC 14
Gecontroleerde toegang op basis van noodzakelijkheid
Volg, controleer, voorkom, corrigeer en beveilig toegang tot cruciale bedrijfsmiddelen (zoals informatie, resources, systemen) volgens de formele bepaling van welke personen, computers en toepassingen toegang nodig hebben en recht op toegang hebben tot deze cruciale middelen op basis van een goedgekeurde classificatie.

CSC 15
Draadloze toegangscontrole
Volg, controleer, voorkom en corrigeer het beveiligingsgebruik van draadloze lokale netwerken (LAN's), toegangspunten en draadloze cliëntsystemen.

CSC 16
Accountbewaking en -controle
Beheer actief de levenscyclus van systeem- en toepassingsaccounts (d.w.z. het maken, gebruiken en verwijderen van accounts en niet-actieve accounts) om de kans te minimaliseren dat aanvallers er gebruik van maken.

CSC 17
Evaluatie van beveiligingsvaardigheden en de juiste training om hiaten op te vullen
Identificeer de specifieke kennis, vaardigheden en mogelijkheden die nodig zijn om verdediging van de onderneming te ondersteunen; ontwikkel een geïntegreerd plan om hiaten te evalueren, identificeren en verhelpen, en voer dit plan uit, door middel van beleid, organisatorische planning, training en bewustwordingsprogramma's voor alle functierollen in de organisatie.

CSC 18
Beveiliging van toepassingen
Beheer de levenscyclus van de beveiliging van alle in-house ontwikkelde en verworven software om zwakke plekken in de beveiliging te voorkomen, detecteren en corrigeren.

CSC 19
Incidentrespons en -beheer
Bescherm de informatie en reputatie van de organisatie door een incidentresponsinfrastructuur te ontwikkelen en implementeren (zoals plannen, gedefinieerde rollen, training, communicatie, managementtoezicht).

CSC 20
Penetratietests en simulatie-oefeningen
Test de algehele sterkte van de verdediging van een organisatie (technologie, processen en mensen) door de doelstellingen en acties van een aanvaller te simuleren.

AXIANS.NL/OPLOSSINGEN/SECURITY security@axians.com

FORTINET CISCO TREND MICRO vmware SentinelOne VINCI ENERGIES