Cybersecurity by Routz

SEQRIT by Routz

Routz is dé kennisautoriteit op het gebied van IT networking en security. We zijn al meer dan 25 jaar expert op het gebied van connectivity en beveiliging. Sinds 1994 beveiligen we zowel Information Technology (IT) als Operational Technology (OT).

Binnen cybersecurity zijn adviseren en implementeren vaak totaal verschillende werelden. Onze kracht is dat we beide werelden beheersen én weten te combineren. Wij geven advies en ontwikkelen beleid voor cybersecurity. Dat beleid vertalen we naar security roadmaps en concrete acties voor uw organisatie. En als u wilt, voeren we die concrete acties ook uit. Zo heeft u direct werkbare oplossingen.

In alles wat we doen, overheerst klantgerichtheid en pragmatisme. Daarom kunnen onze consultants flexibel worden ingezet, van lange termijn opdrachten tot korte projecten, en in verschillende contractvormen.

Inhoud

Cybersecurity wordt steeds belangrijker

Connectiviteit is onmisbaar, en alles is gekoppeld …

Connectiviteit en informatie zijn onmisbaar voor uw organisatie. Al uw computers zijn met elkaar verbonden, net als de mobiele telefoons en tablets van uw medewerkers. De kans is groot dat u voor ERP-software, CRM-software of dataopslag gebruik maakt van de cloud. Bent u producent, dan kunt u ook uw machines nog aan deze opsomming toevoegen. En dan hebben we het nog niet eens over de koppelingen met leveranciers en afnemers. Of over de apparaten die via internet met elkaar verbonden zijn - het Internet of Things (IoT).

… dat vraagt om een steeds betere en integrale cybersecurity aanpak

Die afhankelijkheid zorgt ook voor kwetsbaarheid. Dagelijks worden nieuwe kwetsbaarheden ontdekt in software en apparaten. Lukt het criminelen om toegang te krijgen tot uw data of apparatuur? Dan kan de gevolgschade groot zijn. De schade door ransomware loopt wereldwijd in de miljarden per jaar – en neemt toe. Losgeldeisen van vele miljoenen euro's per bedrijf zijn geen uitzondering meer. Daarom is cybersecurity zo belangrijk: het beschermt uw organisatie tegen aanvallen en incidenten van buitenaf en binnenuit.

… voor IT- én OT-omgevingen

Bij veel bedrijven is het bewustzijn over IT-security de laatste jaren sterk gegroeid. Maar we zien ook dat het bewustzijn over OT-security daarbij achterblijft. Niet heel gek, want OT wordt vaak gezien als 'stand-alone', machine-gebonden software, die een deel van de productie ondersteunt. De software waarmee productiesystemen en machines worden aangestuurd, is gebouwd om vele jaren mee te gaan. En een aantal jaren geleden werd die software niet ontworpen met informatiebeveiliging in het achterhoofd. En daar ontstaat het probleem. Want die productiesystemen en machines worden inmiddels steeds vaker direct of indirect aan het kantoornetwerk of het internet gekoppeld. En daardoor worden ze ook kwetsbaar voor aanvallen van buitenaf.

Dit is hoe we werken

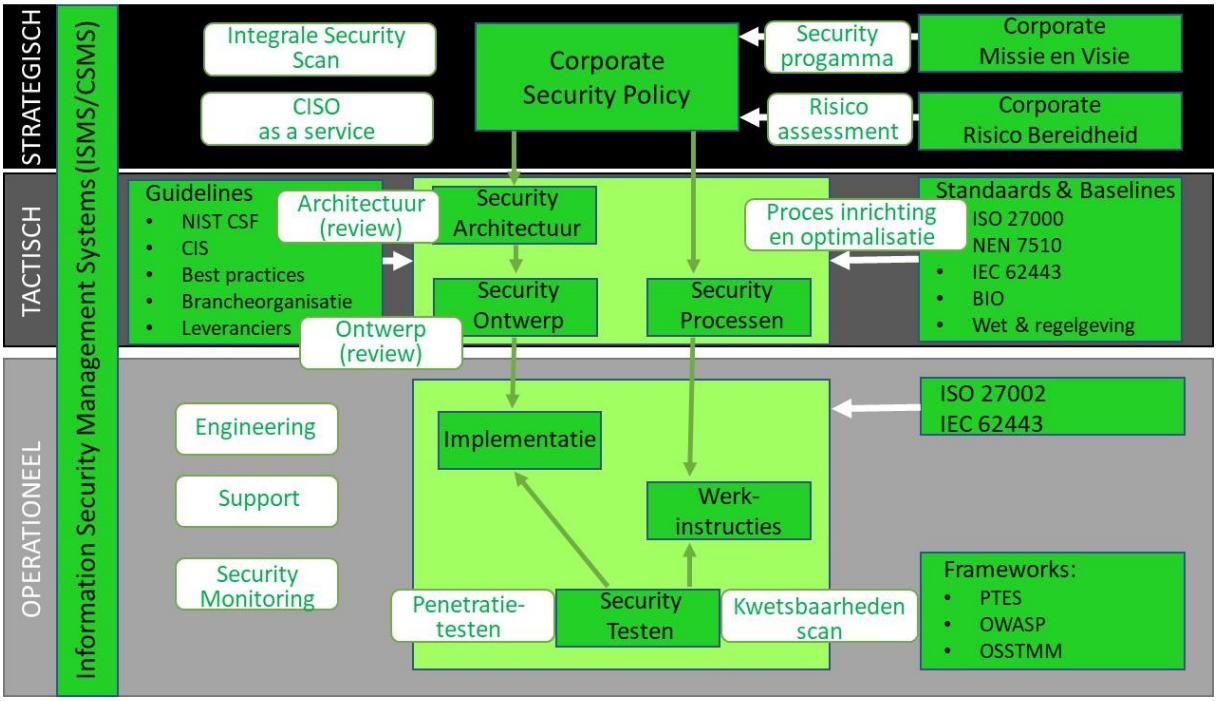
Voorkomen dat uw informatie en informatiesystemen gecompromitteerd worden. Dat is wat we doen. Pragmatisch en no-nonsense. We zijn specialisten in IT- en OT-security, en staan voor advies, implementatie én beheer. Dat doen we met een team van ervaren, hoogopgeleide security consultants.

We brengen overzicht in complexe materie …

Connectiviteit is de hoeksteen geworden van alle IT- en OT-systemen, en dus van uw organisatie. En hoe belangrijker connectiviteit voor uw organisatie is, hoe groter de risico's die ermee samenhangen. Zaak dus om overzicht te bewaren en integraal te werken. Zo helpen we u om security op uw businessdoelen af te stemmen.

… koppelen advies aan implementatie

We geven aan waar en hoe u kunt verbeteren. En als u dat wilt, realiseren we die verbeteringen ook voor u. Zo weet u zeker dat de adviezen uitgevoerd worden door een partij die écht begrijpt wat er moet gebeuren. En dat er niets tussen wal en schip valt.



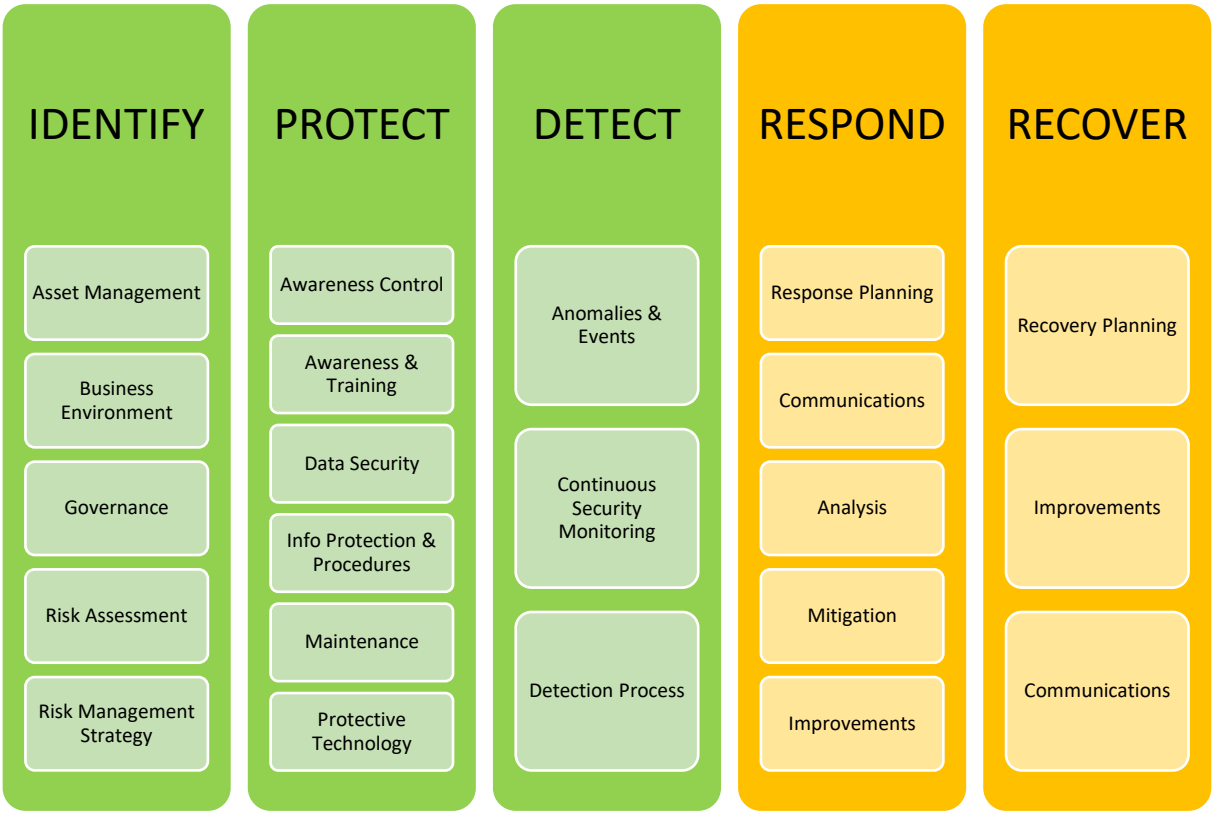
Figuur 1. SEQRIT Ervaring

… hebben óók oog voor uw business

Cybersecurity is ook een afweging tussen kosten en baten. Op basis van de Integrale Security Scan bepalen we samen met u welke maatregelen absoluut noodzakelijk zijn, en welke een lagere prioriteit krijgen. Om die afweging zo goed mogelijk te kunnen maken, brengen we samen met u de kroonjuwelen van uw organisatie in kaart: welke onderdelen moeten absoluut beschermd worden? Vervolgens kijken we heel pragmatisch hoe we dat bereiken met een zo kostenefficiënt mogelijke inzet van security maatregelen.

… en werken met een stevig, bewezen framework

We vinden niet iedere keer opnieuw het wiel uit, maar hanteren het NIST cyber security framework. Dat is een reeks richtlijnen voor het beperken van organisatorische cyberbeveiligingsrisico's, gepubliceerd door het Amerikaanse National Institute of Standards and Technology. Het NIST baseert zich op bestaande normen, richtlijnen en praktijken en is dus heel praktisch toepasbaar. . Voor alle onderdelen van het framework gebruiken we marktconforme standaarden, zoals ISO 27001 en IEC 62443, die naadloos aansluiten op het NIST cyber security framework.



Figuur 2. NIST Cybersecurity Framework Functies

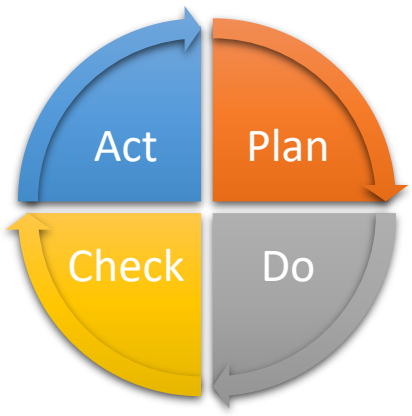
Elke stap volgt logisch op de vorige …

Cybersecurity mag geen papieren tijger zijn. Daarom geldt bij SEQRIT dat elke stap logisch uit de vorige voort moet vloeien. Preciezer gezegd: top down moet herleidbaar zijn dat beleid vertaald is naar processen, procedures en een (technische) implementatie. En bottom up moet bewijsbaar zijn dat de implementatie het beleid dekt. Zo weten we zeker dat er geen licht zit tussen het opgestelde beleid en de daadwerkelijke uitvoering daarvan.

… en security blijft een continu proces

Als we in uw organisatie een Information Security Management System (ISMS) invoeren of reviewen, bewaken we altijd drie dingen. In de eerste plaats dat de geïmplementeerde

maatregelen in lijn zijn met het beleid van uw organisatie. In de tweede plaats dat er geen overbodige maatregelen worden toegevoegd. En tot slot dat alle essentiële beleidspunten in maatregelen vertaald zijn. Beleid leidt zo tot processen, procedures en ontwerpen - en die leiden weer tot implementaties. Die toetsen we, en zo komen we tot eventuele vervolg- en verbeteracties. Dit is een continu proces, dat zich prima laat omschrijven met de kwaliteitscirkel van Deming: *plan, do, check, act*.



Figuur 3. Kwaliteitscirkel van Deming

Plan
Met een risico assessment brengen we de belangrijkste risico's in kaart. Vervolgens selecteren we de benodigde tegenmaatregelen. Voor de implementatie daarvan stellen we een realistisch plan op. Daarbij houden we rekening met urgentie, en met wat uw organisatie aankan.

Do
Dit is de fase waarin de plannen worden gerealiseerd. We stellen processen en procedures op, of verbeteren ze. Waar nodig passen we rol- of functiebeschrijvingen aan. Tools worden aangeschaft, technische verbeteringen uitgevoerd. En daarna implementeren we het geheel.

Check
Meten is weten! Enige tijd nadat we de geplande aanpassingen hebben doorgevoerd, controleren we of het verwachte beveiligingsniveau inderdaad is behaald. Hoe we dit precies meten en bewaken, hebben we in de voorgaande fases al bepaald en ingericht.

Act
Blijkt uit de metingen dat de beveiliging nog niet op niveau is? Dan is dit het moment om correcties uit te voeren. En ook als het gewenste niveau al wél bereikt is, bent u helaas nog niet klaar. Wijzigingen in uw processen of organisatie kunnen leiden tot nieuwe risico's. Net als technologische ontwikkelingen, veranderende wetgeving, andere leveranciers en nieuwe versies van software. Daarom is het van belang om de stappen uit de cirkel van Deming in elk geval eens per jaar te herhalen.

Dit is onze ervaring

U profiteert mee van de ervaring van anderen …

We namen al bij veel verschillende opdrachtgevers in verschillende sectoren de cybersecurity onder de loep. En van die ervaring profiteren al onze opdrachtgevers mee. Bijvoorbeeld omdat we vaak dezelfde aandachtspunten tegenkomen. Daar controleren we inmiddels dan ook bijna standaard op. Het gaat dan onder meer om de volgende punten:

- het ontbreken of niet toereikend zijn van een security beleid;
- een gebrek aan inzicht in kritische data en systemen;
- een gebrek aan actueel inzicht in aard en ernst van risico's;
- een gebrek aan aansluiting tussen beleid en implementatie (bijvoorbeeld een firewall policy die niet herleidbaar is tot de security policy);
- het ontbreken of niet toereikend zijn van standaard beveiligingssoftware of beveiligingsprotocollen;
- het ontbreken of niet toereikend zijn van netwerktoegangscontrole;
- het gebruik van standaard accounts op systemen met persoonsgegevens;
- het gebruik van software of netwerken voor systeembeheerders die makkelijk door buitenstaanders benaderbaar zijn – en dus overgenomen kunnen worden;
- het publiceren van toegangsinformatie op openbare websites;
- het niet of niet overal gebruiken van encryptie voor websites, waardoor verzonden gegevens uitgelezen kunnen worden;
- het gebruik van verouderde en niet meer door de leverancier ondersteunde apparatuur;
- het gebruik van operating systems die verouderd zijn en bekende kwetsbaarheden bevatten;
- het gebruik van firewalls die niet volledig geconfigureerd zijn, waardoor netwerkverkeer soms onterecht wordt doorgelaten;
- het gebruik van firewalls met veel vervuiling in de toelatingsregels, waardoor onduidelijk is of de juiste regels nog actief zijn.

… en van specifieke opdrachten

Hieronder een greep uit het werk dat we in verschillende sectoren al verrichtten.

Nutsbedrijf

Steeds meer in- en externe systemen zijn tegenwoordig aan elkaar gekoppeld. Ook bij nutsbedrijven. Dat maakt ook dat kwaadwillenden mogelijk delen van de nationale nutsvoorzieningen plat kunnen leggen. Om dat te voorkomen, helpen we een nutsbedrijf door het periodiek uitvoeren van kwetsbaarhedenscans en penetratietesten. Als de uitkomsten daar aanleiding toe geven, brengen we adviezen uit – die we ook omzetten naar concrete maatregelen. En de voorgestelde verbeteringen in de netwerkbeveiliging implementeren we ook.

Overheidsorganisatie
Voor een overheidsorganisatie leveren we een gedetacheerde security officer. Die is verantwoordelijk voor de implementatie en uitvoering van het beveiligingsbeleid in het hem toegewezen aandachtsgebied.

Supermarktketen
Voor een supermarktketen hebben we het informatiebeveiligingsbeleid opgesteld. Op basis daarvan hebben we vervolgens ook het programmaplan opgesteld voor de invoering van verbeteringen, en voor het inplannen van interne controles en scans. We zijn permanent betrokken bij het doorvoeren van verbeteringen en het uitvoeren van netwerkscans en penetratietesten.

Financiële dienstverlener
Voor een financiële dienstverlener hebben we intrusion detection ingericht als managed service. Daar doen we ook de bewaking van. Daarnaast beheren we de firewall.

Voor een andere financiële dienstverlener voeren we penetratietests uit op systemen die cruciaal zijn voor de bedrijfsvoering. Dat doen we niet alleen: deze dienstverlener rouleert ons hierbij met andere bekende namen in de markt, om zo een objectief oordeel te waarborgen.

Mediaproducent
Voor een mediaproductie bedrijf hebben we het ISMS opgezet en volledig beschreven. Een deel van de maatregelen zijn door het bedrijf zelf geïmplementeerd, en een ander deel door ons. Ook hebben we het hele netwerk opnieuw ontworpen en geïmplementeerd, zodat het weer aan alle beveiligingseisen voldoet.

Offshore bedrijf
Voor een producent van offshore funderingen pasten we het informatiebeveiligingsbeleid aan en stelden we een securityprogramma op. Namens de klant traden we op als technisch geweten naar de externe beheerpartij van de IT-omgeving. Zo bewaakten we dat de technische oplossingen aansluiten bij het bedrijfsbeleid.

Gaswinningsbedrijf
We ondersteunen een gaswinningsbedrijf met het beheren van de OT-omgeving. We zorgen ervoor dat de OT-infrastructuur van meer dan 20 productielocaties veilig blijft. Daarbij nemen we het technische gedeelte uit handen, en zorgen we dat de beleidsstukken en procedures actueel blijven. Bovendien zien we erop toe dat men zich daadwerkelijk aan deze procedures houdt.

Semiconductor
Voor een producent van semiconductors hebben we een plan opgesteld voor het segmenteren van het OT-netwerk van alle fabrieken wereldwijd. Daarmee kunnen we de impact van een eventueel incident sterk beperken. Onderdeel van deze segmentering is ook het beter scheiden van het OT-netwerk van het IT-netwerk. Onze Routz-collega's ondersteunen bij het aanpassen van de netwerken en de firewalls.

Productiebedrijf
Bij een productiebedrijf hebben we een OT Quick Scan uitgevoerd. Hieruit kwam een groot aantal verbeterpunten naar voren. Samen met de klant hebben we een prioriteitenlijst opgesteld. Nu helpen we deze klant om de prioriteiten aan te pakken. Dat gaat onder meer om het opstellen van beleid, om het opstellen en implementeren van asset management, en om patchmanagement voor OT-systemen.

Voedsel- en diervoederindustrie
Voor een wereldwijd opererende organisatie hebben we een plan opgesteld om de netwerk-infrastructuur op veel productielocaties te moderniseren, en het niveau van security verder te verhogen. We hebben een review uitgevoerd op de bestaande firewall configuraties, een verbetervoorstel gedaan, en geholpen bij het beter inzichtelijk maken van de datastromen in het netwerk. Onze collega's van Routz bieden ondersteunen bij het implementeren van het moderniseringsplan en bij het dagelijks beheer van de nieuwe netwerk-infrastructuur, systemen en firewalls.

Systeemleverancier
We leveren een gedetacheerde security officer aan een systeemleverancier wiens producten worden toegepast in missie-kritische infrastructuren. Onze man is verantwoordelijk voor de implementatie en uitvoering van het beveiligingsbeleid in de organisatie en haar producten. Bij deze organisatie werken we aan beleidsdocumenten en aan de doorontwikkeling van het ISMS. Ook hebben we de IEC 62443 OT cybersecurity-standaard geïntroduceerd.

Provinciale overheidsorganisatie
Voor een provinciale overheidsorganisatie hebben we een advies opgesteld over de IEC 62443 OT cybersecurity-standaard. We focusten ons daarbij op het toepassen van de standaard, het implementeren ervan in de organisatie, en het integreren ervan met de ISO 27001 security-standaard.

Deze kennis hebben we in huis

Bij SEQRIT werken gecertificeerde specialisten op alle besturingsniveaus:

Strategisch

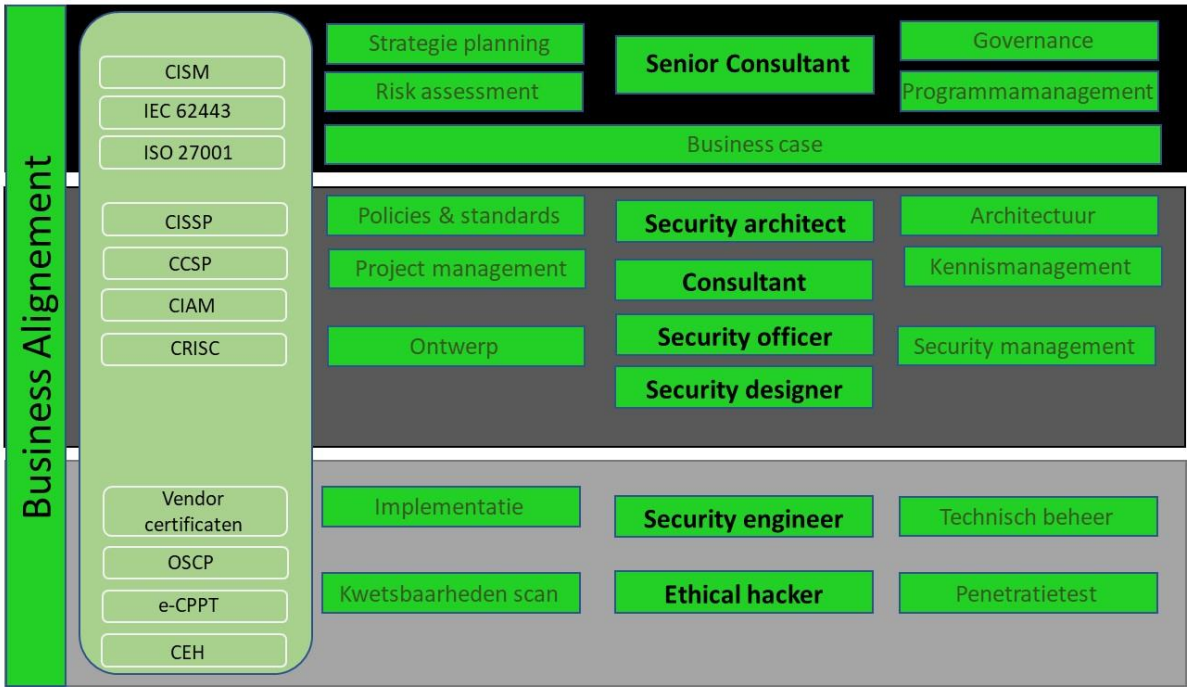
- Certified Information Security Management (CISM)
- IEC 62443
- ISO 27001

Tactisch

- Certified Information Systems Security Professional (CISSP)
- Systems Security Certified Practitioner (SSCP)
- Certified Cloud Security Professional
- Certified Identity and Access Manager
- Certified Risks and Information System Control

Operationeel

- Offensive Security Certified Professional (OSCP)
- Certified Ethical hackers (CEH)
- eLearnSecurity Certified Professional Penetration Tester (eCPPT)



Figuur 4. SEQRIT Kennis