CASESTUDY

Hogere weerbaarheid voor **De Vereende** dankzij beleid en teststrategie

"We wisten al waar onze sterke en zwakke punten lagen, maar de samenwerking met Securify heeft dit naar een hoger niveau getild."

Patricia Koppers, CISO De Vereende

Doelen

- Verhogen weerbaarheid van de organisatie.
- Voldoen aan de eisen van DORA.
- Interne bewustwording over belang van security verhogen.
- Verminderen van risico's door het opvolgen van de bevindingen waarmee de juiste maatregelen worden geïmplementeerd.
- Helder inzicht in de speciefieke cyberrisico's die je als organisatie loopt.

De Vereende is een verzekeringsmaatschappij die oplossingen biedt voor risico's die moeilijk elders onder te brengen zijn en vervult daarmee een vangnetfunctie. Waar de reguliere verzekeraars het risico te hoog vinden, biedt De Vereende de oplossing. Dankzij hun specialistische kennis en klantgerichte aanpak, speelt De Vereende een cruciale rol in het waarborgen van dekking voor uiteenlopende en complexe risico's in de markt.

Uitdagingen

De Vereende is afhankelijk van de integriteit en betrouwbaarheid van haar IT-systemen. De aard van hun werkzaamheden brengt met zich mee dat ze omgaan met gevoelige klantgegevens en complexe financiële transacties, wat hen een aantrekkelijk doelwit maakt voor cyberaanvallen.

Met de invoering van de Digital Operational Resilience Act (DORA) moeten financiële instellingen voldoen aan strenge eisen op het gebied van risicobeheer, incidentrapportage en het testen van de operationele veerkracht. Vanwege de omvang hoeft De Vereende niet te voldoen aan de zwaarste eisen, maar volgen zij wel de richtlijnen om een hoge weerbaarheid te realiseren. Om deze uitdagingen het hoofd te bieden, werkt De Vereende samen met Securify- preventieve cyber security experts.

Cybersecurity en DORA

Onder DORA worden financiële instellingen verplicht om regelmatig security assessments uit te voeren. Hiervoor werkt De Vereende samen met Securify. Het testprogramma van de Vereende bestaat uit verschillende typen testen en activiteiten waaronder pentesten en Purple Teaming sessies.

CASESTUDY

“Een goed securitytestbeleid is een randvoorwaarde. Als organisatie moet je zelf de doelen stellen en samen met de testers bepalen wat je wilt doen”

Veruschka Kavelaars, ISO De Vereende

Oplossingen

1. **Pentesten:** Securify voert regelmatig penetratietesten uit om de weerbaarheid van de systemen van De Vereende te testen en kwetsbaarheden te identificeren.
2. **Purple Teaming Oefeningen**: Door realistische aanvalssimulaties helpt Securify De Vereende om hun operationele weerbaarheid verder te versterken.
3. **Strippenkaart:** Advies en hulp op afroep, waarbij Securify de juiste kennis en inzet op het juiste moment levert.

Patricia Koppers, Chief Information Security Officer (CISO) bij De Vereende, benadrukt het belang van deze samenwerking: “Ik vind het terecht dat pentesten zijn opgenomen in DORA; het is een van de belangrijkste maatregelen. We wisten al waar onze sterke en zwakke punten lagen, maar de samenwerking met Securify heeft heeft onze security naar een hoger niveau getild”.

Samen met Securify stelde De Vereende een roadmap en teststrategie op. Een Business Impact Analysis (BIA) identificeerde de kritische applicaties, zoals de portalen met een koppeling naar de back office. De BIA classificeert deze applicaties volgens de BIV (Beschikbaarheid, Integriteit en Vertrouwelijkheid). Op basis hiervan werd de teststrategie opgesteld.

Securityteststrategie en implementatie

Veruschka Kavelaars, Information Security Officer bij De Vereende, benadrukt: “Een goed testbeleid is een randvoorwaarde. Als organisatie moet je zelf de doelen stellen en samen met de testers bepalen wat je wilt doen. Vervolgens bewandel je samen dat pad en behaal je uiteindelijk het resultaat.” Voor een van de testen werd door De Vereende een realistisch scenario gevolgd zoals een hacker zou handelen. Een phishing test werd opgezet om inloggegevens te verzamelen en deze te gebruiken om in de omgeving in te breken.

“We hebben Securify een laptop gegeven met minimale rechten om te kijken hoe ver ze konden komen,” legt Kavelaars uit. “Gelukkig werd er in onze eigen organisatie goed gereageerd. De partij die onze SOC/SIEM monitoring doet, hadden we niet geïnformeerd, maar ze alarmeerden ons direct toen ze de activiteit opmerkten.”

Purple Teaming

Securify voerde ook Purple Teaming sessies uit, waarbij verdedigers en aanvallers fysiek bij elkaar zitten. Dit maakt het proces interactiever en draagt bij aan het leereffect. “Tijdens deze sessies behandelen we eerst de theorie en brengen we later in de praktijk hoe een hacker te werk gaat en welke acties en stappen er bij ons in de omgeving zijn uitgevoerd,” aldus Kavelaars. “We hebben deze sessies gedaan met technische teams, IT-teams en het security team, evenals een team van twintig medewerkers op andere niveaus in IT.”

Patricia Koppers onderkent het belang van deze sessies: “Na een tijdje kan het gebeuren dat het security aspect gebagatelliseerd wordt. Dan gebruiken we de voorbeelden van de tests en de Purple Teaming. Ook haken we Securify weer eens aan om iets toe te lichten.”

Resultaten

- Hogere weerbaarheid van De Vereende, gebaseerd op de organisatie en IT-omgeving, tegen cybercriminaliteit.
- Hoger security-bewustzijn binnen de organisatie.
- Voldoen aan DORA richtlijn met betrekking tot pentesten.

Over Securify

Securify biedt geavanceerde preventieve security-oplossingen om de weerbaarheid van organisaties, infrastructuren, applicaties en code te versterken. Onze ruim 45 professionals hebben meer dan 200 jaar gezamenlijke ervaring in security. Ze hebben honderden organisaties ondersteund met duizenden code reviews en pentests, variërend van basis-beoordelingen tot complexe “red en purple team”-opdrachten en het nabootsen van geavanceerde aanvallen als statelijke actoren.

In 2021 verwierf Solvinity een meerderheidsbelang in Securify, waardoor Securify waarde kan toevoegen aan de gemanagede IT-diensten van Solvinity. Securify blijft daarnaast onafhankelijkheid behouden om als technische expert de staat van preventieve security in uiteenlopende sectoren te verbeteren.

Resultaten en continue verbetering

Het uitgangspunt is altijd dat de organisatie opvolging geeft aan de bevindingen. De rapportages van Securify bevatten niet alleen bevindingen, maar ook adviezen en mogelijke oplossingen. “De rapportages zijn uitgebreid en laagdrempelig, voor iedereen begrijpelijk,” zegt Koppers. “Het is duidelijk wat er moet gebeuren en nadat je de bevindingen hebt opgelost moet je nóg een keer hertesten om zeker te weten dat je je weerbaarheid hebt verhoogd.”

Securify communiceert helder op zowel management als technisch niveau. “Voor de technische mensen gaan ze de diepte in, en voor het management leggen ze op een andere manier de vinger op de juiste plek,” merkt Kavelaars op. “We kunnen Securify altijd bellen als we ze nodig hebben, hiervoor hebben we een strippenkaart. Dit kwam ons goed van pas toen we ontdekten dat er een hacker in de omgeving zat. Securify had tijdig door wat er gebeurde en gaf advies over hoe we de hacker eruit konden werken.”

Conclusie

De samenwerking met Securify heeft De Vereende geholpen hun digitale weerbaarheid significant te verhogen. Er zijn verschillende securitytesten op verschillende niveau’s afhankelijk van het doel en de volwassenheid van de organisatie. Door regelmatig pentesten en purple teaming sessies uit te voeren, zal De Vereende voldoen aan de DORA-eisen en beschermt het zijn kritieke IT-systemen tegen cyberdreigingen.

Patricia Koppers concludeert: “Wij zijn in de lead, wij moeten dat doel van de testen bepalen. Securify geeft daarbij adviezen om de samenhang van de testen te borgen en ervoor te zorgen dat we ons uiteindelijke doel halen. Het is een leerproces voor de hele organisatie. De rapportages van Securify zijn voorzien van duidelijke bevindingen en van praktische adviezen. Door het verhogen van het bewustzijn hebben we onze organisatie ook weerbaarder gemaakt. Medewerkers denken nu meer vanuit een securityperspectief.”
De samenwerking met Securify blijft van cruciaal belang voor De Vereende om de digitale weerbaarheid te handhaven en voortdurend te verbeteren.