IP4Sure heeft de pentest voor Please Payroll succesvol afgrond

HR-specialist Please liet webapplicatie pentesten door IP4Sure

Please IP4SURE CYBER SECURITY.

De Helmondse specialist in personeelszaken en werkgeverschap Please, zorgt er al sinds 2000 voor dat ondernemers zich kunnen richten op waar ze goed in zijn: ondernemen. Zij verzorgen niet alleen de personeels- en salarisadministratie van ongeveer 1.000 verschillende opdrachtgevers, maar eigenlijk alles wat met werkgeverschap te maken heeft. Waar het personeel van Please in de begindagen nog veel gegevens handmatig moest verwerken, is nu een heel groot deel van de werkzaamheden geautomatiseerd met slimme software en een uitgebreide webapplicatie.

Hier kunnen werknemers en opdrachtgevers terecht voor uiteenlopende zaken, zoals hun urenadministratie, loonstrookjes, management-informatie, contractverleningen, vragen en nog veel meer. In dit systeem staan natuurlijk veel privacygevoelige gegevens en gebruikers moeten ervan verzekerd zijn dat deze gegevens optimaal beveiligd zijn. In het kader van 'de slager moet zijn eigen vlees niet keuren', schakelde Please cybersecurityspecialist IP4Sure in voor een uitgebreide penetratietest.

De webapplicatie UurOnline was in 2005 het eerste urenportaal in Nederland. Hoewel het ooit begon als een urenregistratiesysteem, dekt de naam de lading allang niet meer. Inmiddels is de door Please zelf ontwikkelde applicatie een volledig online personeelsdossier, waarin werknemers en werkgevers alle personeelszaken terug kunnen vinden. Van urenregistratie tot loonstroken en van contracten tot jaaropgaven. "Het is eigenlijk een volledig personeelsadministratiesysteem," vertelt Hans van de Ven, Algemeen Directeur van Please. "Onze filosofie is dat je terecht moet kunnen bij één loket en één contactpersoon voor al je werkgerelateerde zaken. Er zijn iets meer dan 800.000 kleine werkgevers in Nederland, die bij elkaar de grootste werkgever van Nederland zijn. Die hebben meestal niet de beschikking over een HR-afdeling of specialisten op het gebied van arbeidsovereenkomsten of salarisadministratie. Deze bedrijven willen we ontzorgen, door de gespecialiseerde partner te zijn die ze nodig hebben."

Please

IP4SURE
CYBER SECURITY.

Meer dan 15.000 actieve gebruikers

UurOnline wordt op dagelijkse basis geraadpleegd door meer dan 15.000 actieve gebruikers, die erop moeten kunnen vertrouwen dat hun gegevens veilig zijn en dat de applicatie voldoet aan de eisen die de Europese privacywet, de AVG, stelt. En niet alleen de gebruikersinterface moet waterdicht zijn, ook de externe systemen van opdrachtgevers, die via een API gegevens uitwisselen met UurOnline, moeten dat op een veilige manier kunnen doen. Hoewel Please over een professioneel team van developers beschikt, dat veiligheid hoog in het vaandel heeft, besloot het bedrijf om de ultieme beveiligingstest uit te besteden aan een partner.

"Wij gaan heel secuur om met de gegevens die klanten ons toevertrouwen. Niet alleen wijzelf willen zeker weten dat onze beveiliging strenge tests doorstaat, ook onze opdrachtgevers willen bewijs zien dat onze systemen zo veilig zijn als wij beweren," stelt Van de Ven. "Ze vragen bijvoorbeeld naar het laatste pentestrapport en dat mag vaak niet ouder zijn dan een jaar, of liever: zes maanden. Logisch, want de software wordt voortdurend bijgewerkt, waardoor er altijd nieuwe beveiligingsrisico's kunnen ontstaan. En dan gaat het niet alleen om de software die we zelf ontwikkelen, maar ook over software van derden. Wij gebruiken bijvoorbeeld Microsoft Web Services en de updates die Microsoft uitrolt, kunnen ook beveiligingsrisico's op ons platform introduceren. Dat wil je regelmatig laten testen."

Waarom IP4Sure?

Er waren al gesprekken gevoerd met verschillende grote security-specialisten, maar dat leidde niet tot de gewenste uitkomst. "Die vonden ons eigenlijk te klein," vertelt Van de Ven. "Al voor we een afspraak hadden gemaakt, kregen we vragen als: wat is jullie budget? Ik zei dan: ik heb geen specifiek budget, ik wil gewoon de zekerheid dat de applicatie op alle fronten getest wordt. Als je vanuit een beschikbaar budget denkt, geef je de klant niet het gevoel mee te denken over wat er echt nodig is. Ik voelde de klik niet. Toen kreeg ik een mailing van IP4Sure in mijn inbox, over een kennissessie die zij gaven. Ik kende Twan Wouters, een van de oprichters, nog uit de tijd dat hij ons IT-support gaf en die samenwerking was altijd goed bevallen. Ik ben naar de kennissessie gegaan en legde hen mijn vraag voor. In dat eerste gesprek kreeg ik direct het vertrouwen waar ik naar op zoek was. IP4Sure voelde als een specialist die niet in budgetten dacht, maar in security-vraagstukken. En dat gevoel bleek juist."

> "Wij gaan heel secuur om met de gegevens die klanten ons toevertrouwen."
>
> - Hans van de Ven, Algemeen Directeur van Please

Met vlag en wimpel geslaagd

Van de pentest zelf heeft Please weinig gemerkt: "We hebben ons datacenter van tevoren ingelicht dat er getest zou worden, want je wil natuurlijk niet dat ze poorten blokkeren en het reguliere verkeer er last van heeft. De applicatie werd heel uitgebreid onderzocht door IP4Sure. Er is bijvoorbeeld gekeken of er zonder login ingebroken kon worden en of je met een bepaalde identiteit ook bij gegevens kon komen waarvoor je geen rechten hebt. We zijn gelukkig met vlag en wimpel geslaagd: van de kritieke doelen is er geen behaald. Goed nieuws dus voor onze developers. Er waren wel wat kleine issues die een minimaal risico vormden, want die vind je nou eenmaal altijd, maar in het rapport gaf IP4Sure heel duidelijk aan hoe we die snel konden verhelpen, inclusief links naar relevante artikelen over het onderwerp. Je leert er dus ook nog wat van!"

Een echte partner

Van de Ven is zeer te spreken over de samenwerking met IP4Sure. "Ik ben zelf van huis uit automatiseerder, dus goed in staat om te bepalen of een partner wel genoeg van de materie weet. Ik kan met zekerheid zeggen dat de mensen van IP4Sure echt specialisten zijn op hun gebied. Ze kijken bovendien goed met wie ze te maken hebben en welke aanpak daarbij past. Ze gingen bijvoorbeeld vooraf met onze developers in gesprek om te bepalen wat er wel en niet getest moest worden, zodat er meer tijd was om de relevante zaken te testen. Dat is heel wat anders dan simpelweg vragen wat ons budget is. Er is wel een mooie parallel te trekken met onze eigen dienstverlening. Door een partner als IP4Sure zijn wij in staat om ons te focussen op waar we goed in zijn. Net als bedrijven hun personeelsadministratie aan ons uitbesteden, besteden wij het testen van onze webapplicatie uit aan een specialist die we vertrouwen. En net als wij geen leverancier-afnemer-relatie met onze klanten willen, zoeken we zelf ook externe specialisten die echt een partner voor ons kunnen zijn."

Please IP4SURE CYBER SECURITY.