Blijf beveiligingsproblemen voor met tijdige informatie en actie

In het voortdurend veranderde digitale landschap van nu worden bedrijven van elke omvang doorlopend bedreigd door inbreuken op hun cyberbeveiliging. Volgens het Cybersecurity Infrastructure Security Agency (CISA) wordt 50% van de bekende misbruikte kwetsbaarheden binnen twee dagen na ontdekking misbruikt en 75% binnen een maand. Daarom is het essentieel om snel maatregelen te kunnen treffen voordat kwaadwillenden het netwerk van de organisatie kunnen binnendringen en meer schade kunnen aanrichten.

Dynamische kwetsbaarhedendetectie

In het kader van ons Vulnerability Management Outreach-programma bewaakt, scant en identificeert ons Cyber Intelligence Team stelselmatig kwetsbaarheden en nieuwe kritieke bedreigingen om onze verzekeringnemers te beschermen. Verzekeringnemers die zich aanmelden voor meldingen, worden geïnformeerd via:

Ons Outreach-programma - Cyberverzekeringnemers krijgen bericht als er bekende kritieke kwetsbaarheden in hun omgeving worden aangetroffen die hoogstwaarschijnlijk zullen worden misbruikt.

- Het eerste bericht wordt via e-mail verzonden en bevat details over het risico en de maatregelen die voor herstel nodig zijn.
- Follow-up vindt via e-mail en telefonisch plaats.

Belangrijke meldingen - Deze worden verstuurd naar cyberverzekeringnemers wanneer nieuwe kwetsbaarheden worden ontdekt die hoogstwaarschijnlijk zullen worden misbruikt en die invloed op hun omgeving kunnen hebben.

- Een e-mailbericht met informatie over de nieuwe bedreiging wordt over het algemeen binnen 24 uur na ontdekking verzonden.

Aanvullende Cyber Vulnerability Management-oplossingen

Naast ons Vulnerability Management Outreach-programma kunnen alle Chubb-cyberverzekeringnemers zich inschrijven voor de volgende gratis cyberdiensten:

- **Externe kwetsbaarhedencontrole** - In samenwerking met BitSight kunnen verzekeringnemers cyberrisico's in de dagelijkse metingen van hun beveiligingsprestaties opnemen. Hiervoor is een platform beschikbaar dat aan de hand van kritieke meetgegevens zowel sterke als potentiële zwakke punten aangeeft, wat inzicht in de beveiliging van hun organisatie geeft.

Om u in te schrijven voor het Chubb Vulnerability Management Outreach-programma en meer informatie te krijgover de cyberdiensten van Chubb, gaat u naar www.chubb.com/benelux-nl/cyber-diensten-in-de-benelux.html

Vulnerability Outreach Programme van Chubb

Veel gestelde vragen over rode-vlagwaarschuwingen

Algemeen Veelgestelde vragen

Wat is het doel van het Chubb Vulnerability Outreach-programma?

- Het doel is om organisaties te informeren over hun blootstelling aan kwetsbaarheden met een hoog risico en andere ernstige misconfiguraties (open poorten, malware-infecties, enz.). Chubb heeft deze benadering gevolgd om verzekeringnemers te waarschuwen en te helpen bij het identificeren en oplossen van problemen die te maken hebben met het internet die door ons 'threat intelligence'-team worden geclassificeerd als blootstellingen met een hoog risico. Als zodanig kan en zal elk van de kwetsbaarheden die we identificeren door kwaadwillenden worden geïdentificeerd. Bovendien, de lijst van kwetsbaarheden waarop Chubb scant, worden beschouwd als zeer exploiteerbaar.

Waarom waarschuwt Chubb mij voor kwetsbaarheden in mijn omgeving?

- Dit is een belangrijk onderdeel van de symbiotische relatie van Chubb en haar verzekeringnemers. We bieden onze verzekeringnemers al meer dan honderd jaar risicopreventiediensten aan over de hele wereld, wat onze verzekeringnemers betere risicobeheerders maakt, en Chubb een betere verzekeraar. De Cyberpolis is daarin niet anders. Bij het identificeren van kwetsbaarheden die schade veroorzaken en/of op cyberinformatielijsten met hoogrisicobedreigingen staan, maken wij ons sterk om de blootstelling van onze vezekeringnemers aan deze kwetsbaarheden te verminderen.

Hebben deze waarschuwingen een impact op de dekking?

- Nee. Maar, een onwil om actie te ondernemen om deze geprioriteerde kwetsbaarheden te verhelpen, kan echter gevolgen hebben voor de acceptatie van uw polis in de toekomst. Als we bijvoorbeeld deze kwetsbaarheden zien maar de verzekeringnemer niet reageert of geen actie onderneemt, kunnen we overwegen om de dekking niet te verlengen.

Is dit een penetratietest?

- Dit is geen penetratietest. Er is geen actief scannen of pogingen om uw omgeving te infiltreren. Dit proces maakt gebruik van externe passieve scanplatforms die gebruikmaken van een combinatie van open-source intelligentie (OSINT) en passief scannen. Passief scannen is niet-opdringerig en een veilige methodologie om op internet gerichte activa en potentiële kwetsbaarheden of misconfiguraties in verband daarmee te identificeren.to identify internet-facing assets and any potential vulnerabilities or misconfigurations associated with them.

Veel gestelde vragen over rode-vlagwaarschuwingen

Waarom ontvang ik dit?

- U ontvangt deze waarschuwing omdat u zich hebt geregistreerd voor het Chubb Vulnerability Outreach-programma, dat beschikbaar is voor onze verzekeringnemers als een aanvullende dienst bij hun cyberpolis. Het heeft betrekking op een bekende geëxploiteerde kwetsbaarheid (CVE) of elk ander ernstige cyberbeveiligingincident dat werd gedetecteerd via niet-opdringerige externe scantools zoals BitSight en Security Scorecard. De waarschuwing bevat informatie die het IT-team van de verzekerde kan gebruiken om het blootgestelde actief te identificeren en te corrigeren.

Wat als ik deze waarschuwingen niet begrijp?

- Het Cyber Intelligence Team van Chubb bespreekt dit proces en de waarschuwingsgegevens graag met iedereen in uw organisatie. U kunt ze ook doorsturen naar uw interne informatiebeveiligingsprofessional of een externe beheerde serviceprovider die toezicht houdt op uw omgeving voor verduidelijkingen en/of inzichten.

Ik weet niet wat dit is of wat ik eraan moet doen, kunt u helpen?

- Ja, u kunt een verzoek tot algemene ondersteuning aanvragen bij het Cyber Risk Advisory Team van Chubb door contact op te nemen met Cyber@chubb.com
- Zorg ervoor dat u een opmerking toevoegt die aangeeft dat u een kwetsbaarheidsmelding hebt ontvangen en dat u deze wilt bespreken.

Dit is niet mijn IP-adres. Is er actie nodig?

- Gelieve de waarschuwing door te sturen naar Cyber@Chubb.com met vermelding van de specifieke, verkeerd toegekende IP-adressen en wij zullen onze gegevens bijwerken waaruit blijkt dat deze betrekking hebben op een niet-verzekerd object. Indien geïnteresseerd, kan het Chubb Cyber Risk Advisory-team instructies geven aan uw IT-team om een vraag in te dienen voor deze bevindingen via Bitsight of Security Scorecard om toekomstige geautomatiseerde waarschuwingen met betrekking tot deze verkeerd toegewezen IP's te voorkomen.

Dit is niet mijn domein.

- Neem contact op met Cyber@Chubb.com met de bevestiging van het juiste domein en Chubb zal ervoor zorgen dat uw polis wordt bijgewerkt met de juiste gegevens. Vervolgens zullen wij onze administratie bijwerken om aan te tonen dat de kwetsbaarheid betrekking heeft op een niet-verzekerd object en de daarmee verband houdende zaak afsluiten.

Alle cyberdiensten zijn onderhevig aan wijzigingen. Eventuele wijzigingen in het dienstenaanbod worden weergegeven op het lokale webformulier voor cyberdiensten. Verzekeringsnemers zijn verantwoordelijk voor het controleren van de specifieke voorwaarden van elke cyberdienstverlener om in aanmerking te komen en op de hoogte te blijven van eventuele wijzigingen die zich kunnen voordoen.

MET KORTING AANGEBODEN CYBERDIENSTEN DOOR DERDE PARTIJEN:
Externe kwetsbaarheidsmonitoring, Veilige wachtwoordbeheerder
De bovengenoemde cyberdiensten worden door derde partijen aangeboden aan Chubb-verzekeringsnemers voor de genoemde initiële periode, mits de verzekeringsnemer een nieuwe abonnee/klant is van de aangeboden cyberdiensten door de gekozen derde partij en de verzekeringsnemer voldoet aan de gestelde eisen. Na afloop van de genoemde initiële periode hebben verzekeringsnemers de mogelijkheid om hun cyberdiensten voort te zetten tegen een gereduceerd tarief bij verlenging. Houd er rekening mee dat de specifieke korting kan variëren per product en dienst. Kortingen op producten en diensten die worden aangeboden door cyberdienstverleners zijn alleen beschikbaar voor Chubb-verzekeringsnemers met lopende polissen en zijn onderhevig aan de toepasselijke verzekeringswetten. De producten en diensten die worden geleverd door derde partijen worden beheerst door contractvoorwaarden die de verzekeringsnemer aangaat met de derde partij. Chubb is niet betrokken bij de beslissing van de verzekeringsnemer om diensten aan te schaffen en is niet verantwoordelijk voor producten of diensten die worden geleverd door derde partijen.

Wij maken gebruik van door u aan ons [of, voor zover van toepassing, aan uwverzekeringstussenpersoon] verstrektepersoonsgegevensvoordeacceptatie,polisadministratie, schadebeheer, en andere verzekeringsdoeleinden zoals naderomschreven in ons Algemeen Privacybeleid, dat hier kan worden ingezien: www.chubb.com/benelux-nl/footer/privacy-policy.html

Wij maken gebruik van door u aan ons [of, voor zover van toepassing, aan uwverzekeringstussenpersoon] verstrektepersoonsgegevensvoordeacceptatie,polisadministratie, schadebeheer, en andere verzekeringsdoeleinden zoals naderomschreven in ons Algemeen Privacybeleid, dat hier kan worden ingezien: www.chubb.com/benelux-nl/footer/privacy-policy.html