At-a-Glance

Het Cisco-netwerk als handhaver

Gebruik netwerksegmentatie voor risicobeheersing

Uw netwerk wordt voortdurend blootgesteld aan geavanceerde cyberaanvallen door professionele hackers, terwijl het aantal internetverbindingen met de minuut groeit. Elke netwerkverbinding, of deze nu tot stand wordt gebracht via cloud-services, mobiliteit, het Internet of Things (IoT) of iets anders, biedt een mogelijk toegangspunt voor een aanval. Aan u de uitdaging om een goed evenwicht te vinden tussen netwerktoegang voor gebruikers en apparaten en risicobeperking.

Het goede nieuws is dat uw Cisco®-netwerk hier al de juiste middelen voor bevat. U hoeft deze slechts nog te activeren, waarna uw netwerk fungeert als handhaver van het netwerkbeveiligingsbeleid. U kunt bijvoorbeeld bedreigingen indammen door met behulp van Cisco TrustSec® en de Cisco Identity Services Engine (ISE) uw netwerk op te delen in kleinere segmenten. Dankzij een software-gedefinieerde benadering van netwerksegmentatie kunt u de segmenten vervolgens beschermen met behulp van specifiek groepsbeleid dat de gebruikerstoegang bepaalt aan de hand van gebruikersrollen en de bijbehorende bedrijfsbehoeften.

Het resultaat? Veilig beheer van de netwerktoegang op basis van rollen en onafhankelijk van de topologie en toegang. Het mogelijke aanvalsgebied wordt hierdoor sterk gereduceerd. Zelfs als het hackers lukt om uw netwerk binnen te dringen, dan kunnen ze niet langer vrijuit door het netwerk bewegen en wijdverspreid schade aanrichten.

Dynamisch beleid centraal handhaven

Terwijl uw Cisco-netwerk fungeert als handhaver van de netwerkbeveiliging, kunt u uw beveiligingsbeleid centraal toepassen in het gehele netwerk. De juiste gebruikers en apparaten beschikken nu over de juiste toegang en u beperkt de impact van een aanval. Cisco ISE fungeert als de gecentraliseerde beleidsengine die real-time beslissingen voor toegangsbeheer maakt voor switches, routers en beveiligingsapparaten van Cisco.

Daarnaast kunt u de omvang, kosten en complexiteit van de audits voor netwerknaleving volgens de PCI DSS-norm (Payment Card Industry Data Security Standard) en HIPAA (Health Insurance Portability and Accountability Act uit 1996) beperken.

Als u Cisco als een netwerkhandhaver gebruikt, verkleint u de beveiligingsrisico's, verbetert u de operationele efficiëntie van de beveiliging en verbetert u de naleving.

Volgende stappen

Ga voor meer informatie over het gebruik van de oplossing Cisco Network as an Enforcer naar de pagina Cisco Enterprise Network Security.

Gebruik de technologie voor handhaving van beveiligingsbeleid die al in uw netwerk aanwezig is voor het volgende:

- Bedreigingen in uw infrastructuur snel isoleren en beheersen.
- De impact van infiltratie door een aanvaller beperken door uw netwerk te segmenteren.
- Gedetailleerd en consistent toegangsbeheer centraal toepassen voor gebruikers, apparaten, locaties en meer.

“De Cisco-oplossing biedt ons een zeer nauwkeurige manier, vanuit het draadloos access point of de switch, om vast te stellen wie waartoe toegang krijgt. We kunnen gebruikers aan de juiste categorie toewijzen en het juiste beleid instellen om te voldoen aan de eisen voor informatiebeveiliging.”

Roman Scarabot-Mueller
Head of Infrastructure,
Mondi Group International

© 2015 Cisco en/of zijn dochterondernemingen. Alle rechten voorbehouden. Cisco en het Cisco-logo zijn merken of gedeponeerde merken van Cisco Systems, Inc. en/of zijn dochterondernemingen in de VS en andere landen. Ga voor een overzicht van de handelsmerken van Cisco naar: www.cisco.com/go/trademarks. Hier genoemde handelsmerken van derden zijn eigendom van hun respectieve eigenaren. Het gebruik van het woord partner impliceert geen partnerrelatie tussen Cisco en enig ander bedrijf. (1110R)
C45-734478-00 05/15