One-pager

Preventie & detectie van Ransomware

Het aantal ransomware aanvallen steeg vorig jaar met 715%. Deze vorm van malware installeert een kwaadaardig programma waarmee cybercriminelen data kunnen blokkeren voor de rechtmatige eigenaren. Om de gegijzelde bestanden weer vrij te geven moet er losgeld (ransom) worden betaald. In deze one-pager laten we zien hoe Pinewood door middel van security testing en -monitoring (detectie & response) uw organisatie kan wapenen tegen ransomware.

Security Review ter preventie

Allereerst brengen we de kwetsbaarheden in kaart met een “Security Review Ransomware”. Bij de Ransomware Security Review voeren we een risicoanalyse uit met het oog op de dreiging van ransomware en stellen we een adviesrapport op met gepersonaliseerde adviezen en maatregelen. Een risicoanalyse is een belangrijke eerste stap om inzicht te verkrijgen in de kwetsbaarheden die u op korte termijn kunt verhelpen en versterken met de juiste maatregelen. Door uw systemen in een veilige omgeving door security specialisten te laten testen, komen de kwetsbaarheden in uw beveiliging snel naar voren. De Security Review kunt u nog aanvullen met:

- **Continuous Vulnerability Scanning**
  Continuous Vulnerability Scanning scant uw infrastructuur continu op zwakke plekken en kwetsbaarheden. Vanuit ons Security Operations Center (SOC) analyseren, interpreteren en prioriteren onze security specialisten uw informatie. Dit bespaart uw eigen IT-afdeling het zoeken naar deze kwetsbaarheden en geeft hen meer tijd in het oplossen hiervan.

- **Penetratietest (pentesten)**
  Tijdens een penetratietest, of pentest, gaan ethical hackers aan de slag om ingangen te vinden in uw systeem. Ze voeren een veilige, maar realistische, aanval uit op uw IT-beveiliging en kunnen zo zien waar er verbetering nodig is.

Detectie en Response vanuit het Security Operations Center (SOC)

De Security Review is een onderdeel van ons Security Operations Center (SOC) en zoals aangegeven een goede eerste stap. Naast deze preventieve maatregelen is het voor een volledige bescherming tegen cyberaanvallen ook van belang om inzicht te verkrijgen in nog onbekende risico’s, want aanvalstechnieken veranderen continu. Met een Security Operations Center (SOC) wordt uw infrastructuur 24 uur per dag gemonitord tegen nieuwe en evoluerende dreigingen. Onze Security Analisten detecteren, analyseren en beoordelen de dreigingen. Hiermee vermindert u het risico aanzienlijk.

Bij detectie van een (mogelijke) aanval helpen wij u direct met het uitvoeren van een incident response plan om het incident zo snel mogelijk onder controle te krijgen. Zo beschikt u altijd over de juiste expertise en advies over mitigerende maatregelen.

Pinewood doet meer dan testen en monitoring.

Wij ondersteunen bedrijven en instellingen preventief en voeren gesprekken over de risico’s van onder andere malware en hoe die opgevangen dienen te worden binnen uw organisatie. Hiermee slaan we een brug tussen techniek en beleid. Wat doet Pinewood nog meer?

- Training verzorgen op het gebied van awareness/ bewustzijn van medewerkers op het gebied van informatiebeveiliging. • Shared Security Officer.
- Advies geven, ondersteuning bieden of het uitvoeren van een nulmeting voor ISO27001, NEN7510 of een andere gelijkwaardige informatiebeveiligingsnorm.
- Managed Services.
- Ondersteuning bieden bij het opstellen van een informatiebeveiligingsbeleid of -procedures.

pinewood

Over Pinewood

Pinewood is al sinds 1994 een gevestigde naam in de dynamische wereld van de IT-beveiliging. Focus, kwaliteit en samenwerking zijn de kernelementen van onze filosofie. Pinewood focust zich niet exclusief op de technische kant van IT, maar legt altijd de link met uw business. Als zorginstelling betekent dit dat uw informatiebeveiliging in vakkundige en veilige handen is.

Benieuwd naar wat wij voor u kunnen betekenen? Bel ons dan gerust op **015 251 36 36** of stuur een mail naar **info@pinewood.nl**.

Pinewood BV.
Delftechpark 57
2628 XJ, Delft

015 251 36 36
info@pinewood.nl

We see risks
before they hurt