PinkProtect

Checklist beveiliging tegen ransomware & hack aanvallen

Gebruik deze checklist om te toetsen of uw organisatie voldoende is gewapend tegen ransomware en hack aanvallen. De lijst is gebaseerd op de 5 uitgangspunten van het NIST CyberSecurity Framework:

Identificeer	Bescherm	Detecteer	Reageer	Herstel
Breng risico's en dreigingen in beeld	Voorkom dat hackers binnen komen	Voorkom dat hackers onopgemerkt blijven	Voorkom dataverlies, stop aanvallen	Beperk impact op continuïteit

Houd de virtuele deur dicht: veel hack aanvallen vinden plaats omdat basis IT-hygiëne onvoldoende op orde is

- ☐ Zorg dat alle aanwezige systemen en applicaties in beeld zijn, inventariseer nauwkeurig
- ☐ Zorg dat systemen en applicaties altijd zijn bijgewerkt, richt patch management in
- ☐ Zorg dat kwetsbaarheden worden beheerst, richt vulnerability management in
- ☐ Zorg dat malafide software wordt geweerd, gebruik up-to-date anti-malware software en controleer
- ☐ Zorg dat systemen niet onnodig worden blootgesteld, gebruik systeem en netwerk firewalls

Train uw medewerkers: de grootste oorzaak van hack aanvallen zijn medewerkers

- ☐ Zorg voor een informatiebeveiligingsbeleid, stel een gedragscode voor medewerkers op
- ☐ Zorg voor bewustzijn van malafide activiteiten als phishing en social engineering, stel een awareness programma op

Bescherm accounts: de meeste hack aanvallen vinden plaats door misbruik van accounts

- ☐ Zorg voor modern wachtwoord beleid, gebruik unieke wachtwoorden en een wachtwoord-kluis
- ☐ Zorg voor een extra authenticatie middel, gebruik multi-factor authenticatie
- ☐ Zorg voor een extra controle op autorisatie, richt voorwaardelijke toegang in
- ☐ Zorg voor zicht en actie op afwijkingen in login gedrag, richt detectie en protectie in
- ☐ Zorg voor bescherming en registratie van verhoogde toegangsrechten, gebruik een beveiligd toegangssysteem

Bescherm email: de meeste hack aanvallen starten via email

- ☐ Zorg voor het blokkeren van malafide email, gebruik een sterk beveiligde email oplossing
- ☐ Zorg voor het tegengaan van phishing pogingen, gebruik additionele bescherming tegen phishing
- ☐ Zorg voor het beschermen van de identiteit van het maildomein, gebruik anti-spoofing standaarden

Bescherm de IT infrastructuur: de meeste schade ontstaat als een hacker vrij en onopgemerkt kan bewegen

- ☐ Zorg voor voortdurende verificatie van de identiteit van gebruikers en apparaten (Zero Trust principe)
- ☐ Zorg voor het beschermen van de (thuis-)werkplek, richt voorwaardelijke toegang en technisch beleid in
- ☐ Zorg voor het isoleren van kritieke systemen, pas (netwerk)segmentatie toe
- ☐ Zorg voor het kunnen detecteren van malafide activiteiten, gebruik een detectie oplossing

Bescherm data en maak een plan voor herstel: voorkom dat losgeld moet worden betaald

- ☐ Zorg dat afpersing door het lekken van data niet mogelijk is, classificeer en versleutel data
- ☐ Zorg voor een beschermde backup die niet aangetast kan worden, denk ook aan data in de cloud
- ☐ Zorg dat het herstellen van data uit een backup getest wordt, zorg voor voldoende retentie
- ☐ Zorg dat forensisch onderzoek uitgevoerd kan worden, richt logging faciliteiten in
- ☐ Zorg dat de organisatie snel kan herstellen na een succesvolle hack aanval, maak disaster recoveryplannen en test deze periodiek

Heeft u vragen over deze checklist? Wilt u eens praten over het verbeteren van de IT-security binnen uw organisatie? Uw Account Manager kan u verder helpen.