Compliancechecklist voor beveiliging.

Een praktische lijst om endpointapparaten in uw netwerk te beveiligen.

Nieuwe regelgeving vereist dat bedrijven hun focus voor IT-beveiliging verhogen om te waarborgen dat waardevolle klant- en bedrijfsgegevens beschermd worden. Daarnaast vereisen richtlijnen, zoals de EU General Data Protection Reform (GDPR), dat bedrijven veiligheidslekken binnen enkele dagen onderzoeken, monitoren en rapporteren.

Met steeds veranderende regels kan het voor bedrijven een hele uitdaging zijn om tijd en middelen te vinden om bij te blijven. Als ze echter niet meer inzetten dan een eenvoudige firewall tegen aanvallen, kunnen ze worden aangevallen en boetes tegemoetzien die in de miljoenen euro's kunnen lopen. Zonder twijfel zal elk bedrijf eens een aanval of lek meemaken, dus is het essentieel om te identificeren wanneer het gebeurt en dit zo snel mogelijk te corrigeren met de juiste producten, processen en tools.

Deze checklist is een praktische bron voor hen die zoeken naar een verbetering van hun IT-beveiliging en het beschermen van hun merkreputatie, het voorkomen van kostbare gevolgen van een lek en om te voldoen aan strenge nieuwe regels. Start vanaf de basis en werk verder tot maximale beveiligingslagen en u kunt er zeker van zijn dat de beveiliging van uw endpointapparatuur voldoet aan deze strenge nieuwe regels.

Deze handige checklist helpt uw IT-afdeling ook met het beveiligen van hun printers.

Standaard beveiligingsniveau

- Alleen aangekochte apparaten met ingebouwde malwarebeveiliging en versleutelde harde schijven
- Update de firmware, vooral versies met kritische beveiligingspatches, net zoals u dat doet met de apps op uw mobiele telefoon
- Configureer de interfaces van de apparaten en blokkeer protocollen als FTP en telnet als die voor uw toepassing niet nodig zijn
- Beoordeel nieuwe apparaten en sluit poorten of protocollen die momenteel niet in gebruik zijn en indringers toegang zouden kunnen geven
- Pas unieke wachtwoorden voor beheer op elk apparaat toe
- Scherm het bedieningspaneel af om toegang tot beheerfuncties te blokkeren
- Versleutel gegevens van en naar het apparaat
- Stel procedures voor wissen van oude gegevens in, vooral bij printers die u verkoopt

Zodra dit afgerond is, gaat u naar het volgende niveau van beveiliging.

Gemiddeld beveiligingsniveau

- Integreer printer systeemlogdata in uw SIEM-tool om vollediger het netwerk op bedreigingen te kunnen controleren. Voor nieuwe nalevingsregels is overzicht belangrijk om aan de rapportagevereisten te voldoen
- Voer gebruikersauthenticatie in op de printer om bij te houden wie er op het apparaat kopieert, scant en faxt. Deze gegevens zijn handig bij forensisch onderzoek na een inbraak.
- Stel pull-printen in om te voorkomen dat gevoelige informatie wordt achtergelaten. Zo voorkomt u verspilling van papier. Dat is beter voor het milieu.

Zodra dit afgerond is, gaat u naar het laatste niveau van beveiliging.

Geavanceerd beveiligingsniveau

- Stel tracking van printtaken en accountrapportage in
- Overweeg om regels op te stellen en automatisch af te dwingen aangaande wie er toegang heeft tot en gebruik mag maken van printers en waarom met functiegebaseerde authenticatie
- Rol unieke digitale certificaten uit naar elke printer zoals u dat ook bij andere verbonden apparaten op uw netwerk zou doen
- Rol een beheerde mobiele printoplossing uit voor gegevensencryptie, toegang tot apparaten vanaf het netwerk, gebruikersauthenticatie en tracking

4AA7-1093NLE