Bliv klar til det nye NIS2-direktiv fra EU

– det starter med en sikkerhedsscanning af jeres IT-infrastruktur

I efteråret 2024 træder EU's nye reglement for cybersikkerhed, NIS2-direktivet, i kraft. Direktivet stiller krav til, hvordan I som ledelse rapporterer og optimerer virksomhedens sikkerhedsstrategi. Fremover holdes I nemlig direkte ansvarlige for, at virksomhedens cybersikkerhed lever op til de skærpede krav.

Det første skridt mod at opfylde kravene er at få foretaget en grundig scanning af virksomhedens aktuelle sikkerhedsløsninger.

Om sikkerhedsscanningen fra ScanNet

Vi scanner jeres IT med værktøjet Nessus, der er et anerkendt værktøj fra IT-virksomheden Tenable. Ved at scanne alle jeres eksterne IP-adresser og tjenester kortlægger scanningen potentielle risici og sårbarheder. Herefter gennemgår vi rapporten sammen med jeres IT-chef og giver gode råd til, hvordan I imødekommer potentielle sårbarheder og skaber et stærkt værn mod alle de (mange) cybertrusler, som er derude. Her vil vi også kunne rådgive om, hvordan I fremadrettet får en løsning, der sikrer den rette beskyttelse mod cybertrusler.

Det får I ud af en sikkerhedsscanning:

- ✓ **Identificér sårbarheder i jeres IT-infrastruktur**
  Vi identificerer potentielle sikkerhedsrisici i jeres IT-systemer, så I kan gøre noget ved dem, før hackere udnytter eventuelle svagheder.
- ✓ **Gør det muligt at prioritere sikkerhedsindsatser**
  Vores rapport giver en klar oversigt over kritiske sårbarheder, så din virksomhed kan prioritere sikkerhedsindsatsen effektivt.
- ✓ **Sikrer overholdelse af NIS2**
  Scanningen sikrer, at din virksomhed overholder de krav om rapportering og overvågning, der stilles i NIS2-direktivet fra EU.

Sådan booker jeres IT-ansvarlige en sikkerhedsscanning

1.
Scan QR-koden nedenfor, følg dette link eller gå til: https://info.scannet.dk/book-sikkerhedsscanning

2.
Indtast virksomhedens kontaktoplysninger, så vi kan kontakte dig angående en scanning. Vi anbefaler at det er virksomhedens IT-ansvarlige, der noteres som kontaktperson.

3.
Vi vil hurtigst muligt ringe dig op.
For at foretage scanningen, skal vi bruge virksomhedens offentlige IP-adresser og domæner/subdomæner. Dette gennemgår vi nærmere over telefonen.

4.
Når vi indsamler ovenstående, vil vi samtidig stille spørgsmål til jeres nuværende setup, så vi kan rådgive jer på et oplyst grundlag. Derudover booker vi et møde til den endelige gennemgang af scanningen. Du kan forvente dette møde 1-2 arbejdsdage efter den indledende dialog.

5.
Til sidst gennemgår vi rapporten på et onlinemøde og rådgiver (hvis nødvendigt) om tiltag, der kan rette op på eventuelle sårbarheder i jeres IT-systemer.

Første gang, du ønsker at anvende en sikkerhedsscanning fra ScanNet, er både scanningen og konsultationen uden beregning. Produktet kan efterfølgende købes i forskellige løsninger alt efter virksomhedens behov.

Har du spørgsmål, eller ønsker du at høre mere om sårbarhedsscanningen, er du altid velkommen til at kontakte os på Tlf. 75 53 35 00 eller salg@scannet.dk