Underretning om cyberangreb

Til alle interessenter på Kolding HF & VUC

BEMÆRK: Vi er *ikke* et af de VUC 'er, der mistede adgangen til Ludus. Vi har hele tiden haft fuld adgang til systemerne.

Vigtig besked til medarbejdere, tidligere medarbejdere, kursister og tidligere kursister

VUCHosting blev udsat for et større cyberangreb den 9. oktober, hvor vores LUDUS-database blev krypteret af hackere. VUCHosting, som KVUC er værtsinstitution for, hoster LUDUS på 26 VUC' er. Der er sket et databrud, hvor eksterne har haft adgang til databasen.

Vi kan ikke udelukke, at der er sket persondatalæk – derfor denne meddelelse. Det er dog vores klare opfattelse, at sandsynligheden for datalæk som lille, da vores erfarne specialister ikke har fundet tegn på, at der er hentet data ud, og hackergruppen har bekræftet, at de ikke har vores data.

Vi reagerede naturligvis straks på hændelsen og kontaktede med det samme Datatilsynet og Center for Cybersikkerhed. Desuden entrerede vi med meget erfarne professionelle specialister i de efterfølgende dage.

13 af de ramte VUC' er mistede adgangen til LUDUS. Adgangen er nu genetableret efter to uger uden adgang.

Hvilke informationer ligger i den LUDUS-database, der har været hacket?
I LUDUS har vi personoplysninger om alle kursister og medarbejdere, herunder cpr-numre, kontaktoplysninger, eksamensbeviser og dokumentation, der har været relevant for optagelse og gennemførsel. Man kan blandt andet være registreret i LUDUS, hvis man er aktiv som kursist eller medarbejder på VUC, eller hvis man har et eksamensbevis fra VUC, som er udstedt inden for de seneste 30 år.

Hvilke konsekvenser har databrud for mig?
Den specifikke risiko relateret til et datalæk, hvis det har fundet sted, er, at personer med onde hensigter bruger dataene til typisk identitetstyveri eller afpresning. Det kan ikke fuldstændigt udelukkes, at hackere har fået adgang til ovenstående oplysninger.

Hvad har vi gjort efterfølgende for at sikre data?
Vi lukkede straks de angrebne servere ned for at inddæmme angrebet. Vi hentede en database fra backup-serveren, som blev analyseret grundigt for at sikre, at der ikke var inficerede filer. Derefter blev databasen lagt på nye servere hos til LUDUS-leverandøren EG eller IT-fællesskabet ESIS med en fremskyndelse af en allerede planlagt flytning af LUDUS fra VUCHosting. Vi har nulstillet samtlige adgangskoder og brugerne er blevet bedt om at oprette et nyt password, første gang de logger på de nye servere.

Hvad bør du gøre som medarbejder, tidligere medarbejder, kursist eller tidligere kursist?
Som en sikkerhedsforanstaltning opfordrer vi alle til at være ekstra opmærksomme på eventuelle mistænkelige e-mails eller telefonopkald. Hold øje med om du modtager tilbud på f.eks. lån eller kreditkort eller andre handlinger, hvor en anden person kan misbruge dine oplysninger. Skift passwords, hvis du har brugt samme password til flere systemer. Læs mere om internet og sikkerhed på Borger.dk.

Hvor kan jeg få flere oplysninger?
Hvis du har nogen spørgsmål i forbindelse med denne besked, er du velkommen til at kontakte Rektor Anja Pedersen.

Vi beklager meget de gener og bekymringer, det har medført.

Venlig hilsen
Kolding HF & VUC