Microsoft

SVÆRT FOR OFFENTLIGE MYNDIGHEDER AT FINDE NOK RESSOURCER TIL DATASIKKERHED

PÅ TRODS AF MANGE ADVARSLER, EN NY PERSONDATAFORORDNING FRA EU, OG ET STIGENDE ANTAL OFFENTLIGE MYNDIGHEDER, DER BLIVER HACKET ELLER OPLEVER DRIFTSFORSTYRRELSER OG TAB AF DATA, ER DET FORSAT SVÆRT FOR MANGE REGIONER, KOMMUNER OG STATSLIGE INSTITUTIONER AT AFSÆTTE DE NØDVENDIGE RESSOURCER TIL AT BESKYTTE VIRKSOMHEDENS INFRASTRUKTUR, MEDARBEJDERE OG DATA.

For medarbejdere i en kommune med begrænset kendskab til det aktuelle trusselsbillede inden for cyberkriminalitet, forbindes datasikkerhed med en effektiv firewall, backup og antivirus, spamfilter og nogle relevante instruktioner til medarbejderne om håndtering af password, mail og data.
Disse "værktøjer" er stadig meget relevante. Men det er langt fra nok.
Trusselsbilledet flytter sig. Og i takt med, at kommunale medarbejdere kan logge på og arbejde i mange forskellige systemer og apps udenfor kontorets firewall, både på arbejdsgiverens enheder eller egne enheder, har vi gjort det nemmere for hackere at infiltrere vores systemer. Derfor må "værktøjskassen" udvides og processerne om sikkerhed automatiseres. Det kræver flere ressourcer og både strategi og budgetter inden for datasikkerhed må tage højde for dette.
Hackerne bliver stadigt dygtigere – mere professionelle om man vil - og de er langt bedre organiserede i kriminelle netværk end tidligere. Én af de mest hyppige årsager til datatab i en kommune eller offentlig myndighed skyldes brugen af professionelle "Phishing-mails". Problemet med disse falske mails er, at de giver sig ud for at være rigtige mails, og i stadig højere grad ligner modtagerens brugergrænseflade. På den måde lokker afsenderen den kommunale medarbejder til at give brugernavn og passwords via et link til et website. Fordi phishingmailen ligner kommunens egen brugergrænseflade.
Andre phishingmails vedhæfter filer, der ligner et almindeligt Word-dokument, men som reelt indeholder vira. Når medarbejderen åbner linket eller dokumentet, opstår problemerne.

NYE TIDER – NYE VÆRKTØJER

Tidligere kunne en it-organisation beskytte sig mod vira, ved løbende at få opdateret sit antivirusprogram med navnene (signaturen) på kendte vira. Det er ikke længere tilstrækkeligt. Der lanceres i dag nye vira med en hastighed og i et omfang, der gør det svært for selv de mest opdaterede antivirus-databaser at følge med. Desuden skal den traditionelle beskyttelse med opdateringer suppleres af databaser, der ved hjælp af analyser og machine learning, kan vurdere om en fil eksempelvis indeholder kode, der typisk benyttes i malware. I så fald kan mailen og/eller filen blokeres og undersøges nærmere inden den slettes eller frigives.
I andre situationer kommer hackerne ind via svagheder i et ældre system eller gennem en app, en web-applikation eller gennem den enhed, som brugeren anvender til at logge sig på med. Der kan og skal arbejdes på mange fronter for at optimere sikkerheden, men kompromitterede passwords er stadig den største synder og kræver nytænkning, da selv det bedste system ikke kan beskytte organisationen imod en bruger, der af den ene eller den anden årsag mister sit brugernavn og password.

Flere og flere organisationer anvender derfor 2-faktor log-in og/eller biometriske passwords, der gør det sværere for en hacker at udnytte brugerens oplysninger. Andre udvider beskyttelsen af deres brugerdatabaser med intelligente services, der vurderer om vedkommende der logger sig på, opfylder organisationens betingelser til f.eks. lokation, enhed eller browser.
Uanset hvad man gør, er det svært at sikre sig totalt mod at blive kompromitteret, og desværre går der ofte alt for lang tid førend ulovlig indtrængen opdages i organisationens netværk. For at forberede sig på de værste trusler, anvender flere og flere derfor intelligente værktøjer, der kan analysere på en brugers adfærd over tid og derfor opdage ændringer i adfærdsmønstre, der kan tyde på at brugeres identitet er blevet overtaget af en hacker.

Indsamling af data og adfærdsanalyser er overordnet et af de mest effektive våben mod cyberangreb, hvad enten angriberne forsøger eller allerede er kommet ind i organisationens netværk. Microsoft er unik på dette område med bl.a. indsamling og analyse af data via den globale tjeneste "Microsoft Intelligent Security Graph".

Intelligent og automatisk klassificering og beskyttelse af data og dokumenter, kombineret med en struktureret rettighedsstyring på dokument og sagsniveau, er et andet hovedområde hvor offentlige organisationer må sætte ind for at leve op til GDPR og sikre en ansvarlig håndtering af data. Microsoft er også unik på dette område med bl.a. Azure Information Protection , DLP og Azure Rights Management.

MERE AT HENTE

Bliv klogere på udviklingen, aktuelle værktøjer og styr din virksomhed sikkert ind i fremtiden – deltag i et seminar og oplev en live-simulering af sikkerhedsscenarier i innovative omgivelser i Microsofts Technology Center. Læs mere her.

Du kan desuden blive klogere på GDPR og sikkerhed ved at se – eller gense Microsofts webinarer her.

DIGI MES SEN