LogPoints CEO, Jesper Zerlang, kommenterer Center for Cybersikkerheds anbefaling om logning

Oct 19, 2021 15:03 CEST

Nye anbefalinger fra Center for Cybersikkerhed: Sådan styrkes cyberforsvaret mod supply chain-angreb

Center for cybersikkerhed udkom i dag med en rapport, som kortlægger forløbet omkring det omfangsrige SolarWinds-angreb sidste år. Et såkaldt supply chain-angreb, som gennem en kompromittering af it-leverandøren SolarWinds ramte 18.000 organisationer på verdensplan, hvoraf mere end 50 af dem var danske. Center for Cybersikkerheds konklusion er klar: Der er behov for at hæve det generelle sikkerhedsniveau i Danmark.

https://cfcs.dk/da/cybertruslen/rapporter/solarwinds/

Center for cybersikkerhed har tre anbefalinger til danske organisationer:

- Implementering af god logning: Tilbundsgående undersøgelse og analyse af en hændelse
- Beredskabsplan: Sikrer, at hændelser håndteres på en ensartet og systematisk måde.
- Stærkere kontrol med leverandørforhold: Specielt den løbende dialog mellem forretningen og leverandøren er vigtig

LogPoints CEO, Jesper Zerlang, har følgende kommentarer til anbefalingen om logning:

”Center for Cybersikkerhed har helt ret i, at logning understøtter grundig undersøgelse og analyse af en sikkerhedshændelse. Men jeg synes det er endnu vigtigere, at man hele tiden overvåger sine logs og sit netværk, , så man kan stoppe et angreb før det udvikler sig. SolarWinds-angrebet er et glimrende eksempel på, at cyberkriminelle kan have adgang til systemer i månedsvis, før de aktiverer deres angreb. Og her er det langt bedre at kunne opdage dem, inden der sker alvorlig skade.”

”SolarWinds er et såkaldt ’supply-chain’ angreb, hvor hackerne er kommet ind gennem i en ’bagdør’ i SolarWinds-platformen, som producenten uforvarende har distribueret til tusindvis af kunder i hele verden og også i Danmark. Det understreger vigtigheden af at vælge software, som er certificeret efter de højeste sikkerhed- og kvalitetsstandarder som f.eks. Common Criteriea EAL”

”Det er mig magtpåliggende at understrege, hvor vigtigt det er for ledelse og bestyrelse at have et strategisk fokus på cybersikkerhed. Sådan som trusselsbilledet ser ud lige nu, er det ganske enkelt utopisk at tro, man kan holde de cyberkriminelle ude af it-systemerne. Derfor er danske virksomheder nødt til at få styr på, hvad der foregår inden for de digitale mure.”

About Logpoint

Logpoint safeguards society in a digital world by helping customers and Managed Security Service Providers (MSSPs) detect cyberattacks. Combining reliable technology with a deep understanding of cybersecurity challenges, Logpoint makes security operations easier, giving organizations the freedom

to progress. Logpoint's SIEMand NDRtechnologies improve visibility and give a multi-layered approach to cybersecurity that helps customers and MSSPs in Europe navigate the complex threat landscape. Headquartered in Copenhagen, Denmark, Logpoint has a European foundation and is the only European SIEM vendor with a Common Criteria EAL3+ certification. This demonstrates Logpoint's strong focus on data protection and cybersecurity regulations. For more information, visit http://logpoint.com.

Contacts

Maimouna Corr Fonsbøl
Press Contact
Head of PR
PR & Communications
mcf@logpoint.com
+45 25 66 82 98