Hack Day 2019

4. december - Wihlborgs Konferencecenter, Ballerup

08:30 - 09:00	**Registrering og morgenmad**
09:00 - 09:05	**Velkomst** Jakob Schjoldager, redaktør, Computerworld
09:05 - 09:45	**Det aktuelle trusselsbillede** Thorsten Foldager Johnsen, Chef for Trusselsvurderingsenheden, Centre for Cyber Security
09:50 - 10:20	**Cyber incidents? Not on my watch** Philippe Motet Jessen, it-sikkerhedsrådgiver med speciale i awareness, behavior og compliance
10:25 - 10:40	**Pause**
10:40 - 11:15	**Sådan kommer de it-kriminelle ind gennem din indbakke** Jan Kaastrup, CIO & Partner, CSIS
11:20 - 11:55	**Hack dig selv først** Lone Juul Dransfeldt Christensen, Senior Security Architect, Bang & Olufsen
12:00 - 12:45	**Frokost**
12:45 - 13:15	**Virksomhedens menneskelige firewalls** Tobias Andersen, Security Advisor, Institut for Cyber Risk (IFCR)
13:20 - 13:55	**Blockchain og smarte kontrakter vs. hacking: Hvor meget "integritetsbeskyttelse" er for meget?** Søren Debois, Associate Professor, IT-Universitetet i København
14:00 - 14:15	**Pause**
14:15 - 15:00	**En plasticgaffel, et kinesisk kamera og lidt teknisk snilde** Mikkel Holm Brøndum, CEH, OSCP, OSWP – senior analyst, CGI
15:05 - 15:30	**Paneldebat**
15:35 - 15:35	**Opsummering og tak for i dag**

08:30 - 09:00: Registrering og morgenmad

09:00 - 09:05: Velkomst



Jakob Schjoldager
redaktør
Computerworld

09:05 - 09:45: Det aktuelle trusselsbillede

Thorsten Foldager Johnsen
Chef for Trusselsvurderingsenheden
Centre for Cyber Security / Partner

Hør om de største og mest aktuelle cybertrusler i en tid, hvor trusselsbilledet hele tiden ændrer sig i takt med, at hackerne finder nye veje og metoder.

09:50 - 10:20: Cyber incidents? Not on my watch



Philippe Motet Jessen
it-sikkerhedsrådgiver med speciale i awareness, behavior og compliance / Keynote

Styrk sikkerhedskulturen i virksomheden og reducer risikoen for interne databrud og cyberangreb.

Medarbejderne betragtes ofte som virksomhedens svage led, når det handler om informationssikkerhed.

Så hvordan skaber du en kultur, hvor informationssikkerhed bliver lige så naturlig som at spænde sikkerhedsselen i bilen?

I dette oplæg får du et indblik i de ting, som du med fordel kan gøre for at styrke sikkerhedskulturen.

Vi kombinerer de bedste pointer fra adfærdskommunikation og forandringsteori og krydrer det med konkrete eksempler på tiltag, der får medarbejderne til at droppe dårlige vaner til fordel for gode - og sikre - vaner.

10:25 - 10:40: Pause

10:40 - 11:15: Sådan kommer de it-kriminelle ind gennem din indbakke



Jan Kaastrup
CIO & Partner
CSIS / Keynote

Danske virksomheder lænses af CEO-fraud: Mailsvindel koster millioner af kroner

CEO-fraud er blandt de største cybertrusler herhjemme, og politiet modtager dagligt anmeldelser om svindelmetoden. Til forskel fra andre svindeltyper så rammer ceo-fraud alle segmenter, lige fra multinationale selskaber til blikkenslagere og den lokale badmintonklub. Alle kan blive ramt.
Få Jans anbefalinger til, hvordan du bedst muligt kan beskytte din virksomhed mod mailsvindel.

11:20 - 11:55: Hack dig selv først



Lone Juul Dransfeldt Christensen
Senior Security Architect
Bang & Olufsen / Partner

Vi bliver nødt til at tænke sikkerhed ind i alle faser af vores software-udviklingslivscyklus, hvis vi skal sikre vores software mod de cybertrusler, som vi står over for. Med continuous integration og continuous delivery betyder det automatiseringer med værktøjer inden for blandt andet static application security testing (SAST), dynamic application security testing (DAST) og open source analysis (OSA). Men hvilke typer af sårbarheder kan disse værktøjer identificere? Og hvor sikker efterlader de ens software?

Hør om fordelene ved at arbejde med sikkerhed som en integrereret del af DevOps og få indsigt i, hvorfor du stadig bliver nødt til at hacke dig selv først.

12:00 - 12:45: Frokost

12:45 - 13:15: Virksomhedens menneskelige firewalls



Tobias Andersen
Security Advisor
Institut for Cyber Risk (IFCR) / Partner

Dine kolleger er virksomhedens menneskelige firewalls, som både skal patches, konfigureres og gøres robuste til at kunne modstå fremtidens cybertrusler.

I mange år har fokus været på investeringer i tekniske sikkerhedsforanstaltninger. Vi har dog glemt, at det stadig er mennesker, som indkøber, konfigurerer og benytter disse foranstaltninger, hvorfor man risikerer at foranstaltningerne ikke virker efter hensigten, ikke anvendes korrekt eller overhovedet anvendes.

Lær hvordan du kan blive bedre til 'people centric security,' som fokuserer på de menneskelige aspekter inden for it-sikkerhed, der er årsagen til de fleste sikkerhedsbrud. Inden for people centric security tager man udgangspunkt i individet og virksomhedskulturen samt dårlige vaner som drivkraften i implementeringen og anvendelsen af politikker, procedurer samt sikkerforanstaltninger.

13:20 - 13:55: Blockchain og smarte kontrakter vs. hacking: Hvor meget "integritetsbeskyttelse" er for meget?



Søren Debois
Associate Professor
IT-Universitetet i København / Partner

Blockchain og "smart contract" teknologier siges at "fjerne behovet for tillid" eller "fjerne behovet for en troværdig tredjepart". Betyder det, at man ikke skal bekymre sig om at blive hacket, hvis man bruger sådanne teknologier?

Vi præsenterer her cutting-edge forskning i anvendelse af blockchain/"smart contract"-teknologier til kommunal sagsbehandling. Vi skal se, at teknologierne giver integritetsgarantier, særligt beskyttelse mod hacking, i en klasse som det vil være dyrt og besværligt at opnå på anden vis, men at disse garantier kommer på bekostning af fleksibilitet og opdaterbarhed i en grad, som de fleste organisationer ikke vil kunne acceptere.

Resultaterne peger på blockchain (og andre integritets-beskyttelsesmekanismer) som et skridt mod bedre it-sikkerhed, men viser samtidig, hvor vanskelig it-sikkerhed er under krav om kontrollerede opdateringer.

14:00 - 14:15: Pause

14:15 - 15:00: En plasticgaffel, et kinesisk kamera og lidt teknisk snilde



Mikkel Holm Brøndum
CEH, OSCP, OSWP – senior analyst
CGI / Partner

I dette oplæg gennemgår penetrationstester Mikkel Brøndum fra CGI en omfattende opgave fra 2019, som sætter mange af de gængse applikations- og netværksmæssige sårbarheder i en konkret og anskuelig kontekst.

Mikkel tegner og fortæller sig igennem et angreb på en stor produktionsvirksomhed, hvor en plasticgaffel, et kinesisk kamera og lidt teknisk snilde bragte ham ind i virksomhedens allerhelligste fra en pløjemark. Mikkel gennemgår desuden en række relativt simple og lavpraktiske tiltag, som enhver organisation bør overveje at implementere for at højne deres fysiske og logiske sikkerhedsniveau.

15:05 - 15:30: Paneldebat

15:35 - 15:35: Opsummering og tak for i dag