IT FORUM
GRUPPEN

TJEKLISTE:

FORUDSE HACKERENS NÆSTE TRÆK

IT-SIKKERHED

70 100 150 :: KONTAKT@ITF.DK :: ITF.DK

HAR I TJEK PÅ JERES FUNDAMENTALE IT-SIKKERHED?

HVOR SKER DET? HVORDAN OG HVORNÅR?

Er det overhovedet muligt at forudse hackerens næste træk og komme i forkøbet?

Ja – det er det faktisk. Men det kræver, at I gør et grundigt forarbejde. At I lukker de huller, som vi har erfaring for, hackeren vil gå efter.

Har I tjek på jeres fundamentale IT-sikkerhed?

Se spørgsmålene i tjeklisten. **Hvor godt er I sikret?**

1. ER I DET LETTE OFFER?

Cyberkriminelle er konstant på jagt efter et nemt og attraktivt bytte. Ligesom løven, der udser sig det svageste dyr i flokken og sætter et heftigt angreb ind. Er I det lette offer, der virker som en magnet på hackere?

GØR I NOK FOR AT SIKRE, AT DET BLIVER SVÆRERE AT KOMME IND HOS JER?

2. HVEM ELLER HVAD ER DET SVAGESTE LED?

Mange bliver overrasket over, at det kunne ske. "Vi har gjort alt, hvad vi kunne, for at forhindre et angreb, og alligevel står vi nu midt i problemet..." Ingen kæde er stærkere end det svageste led. Tænk på samme måde som hackeren:

ER DER NOGLE STEDER I JERES SETUP, DER FÅR ALARMKLOKKERNE TIL AT RINGE? - FÅ ET IT-SIKKERHEDSTJEK

3. ER JERES MEDARBEJDERE KLÆDT PÅ TIL AT AFVÆRGE ET ANGREB?

I takt med at hackerne bliver mere og mere udspekulerede og maskerer deres angreb som tilsyneladende uskyldige mails, stiger behovet for at være på vagt. IT-sikkerhed handler ikke kun om udstyr og teknik – men i lige så høj grad om at uddanne dine medarbejdere i at være opmærksomme og give dem gode digitale vaner.

HAR I FOKUS PÅ AT GIVE JERES MEDARBEJDERE AWARENESS TRÆNING?

4. VURDERER I RISIKOBILLEDET LØBENDE?

Cyberkriminelle scanner mulighederne konstant, og de ændrer hele tiden strategi. At læne sig tilbage i forvisning om, at forsvarsværket er perfekt, er derfor yderst risikabelt. Det kan godt være, du føler, der er fred og ro: Back-up kører, firewall er aktiv, alle anvender to-faktor-godkendelse, der er øjensynligt ingen angreb... Men så kommer det alligevel – på en ny måde, fra en ny kant...

HVAD GØR I FOR AT FØLGE MED I NYE OG ÆNDREDE RISICI?

5. HAR I DE 18 KRITISKE SIKKERHEDS-KONTROLLER PÅ PLADS?

Når man vil gardere sig mod angreb, er det vigtigt at forholde sig til de standarder, der er på IT-sikkerhedsområdet. En af de standarder, du med fordel kan måle jer op imod, er de 18 sikkerhedskontroller, der er defineret af Center for Internet Security (CIS). Hvis disse kontroller er på plads, bliver det nemmere at forhindre og opdage angreb.

HAR I TAGET STILLING TIL CIS V8? - LÆS MERE HER

6. HAR I EN IT-BEREDSKABSPLAN?

Du har sikkert læst om hackerangreb, der har lagt store, globale virksomheder ned, og hvordan de har kæmpet for at komme op igen. I sådan en situationen, er det helt afgørende, at der er en IT-beredskabsplan. Og det gælder faktisk i alle typer og størrelser af virksomheder. For når alle systemer er hacket, telefonerne ikke virker, hjemmesiden er nede, og kunderne ikke kan få fat i dig, så er det rart at have en plan, som kan "trækkes op af skuffen", og som alle kender.

HAR I EN IT-BEREDSKABSPLAN?

7. HVORDAN OPNÅR I DET RIGTIGE BESLUTNINGSGRUNDLAG?

De fleste har behov for assistance til kampen mod hackerne, for man kan jo ikke være ekspert på alle områder. At følge med i den hastige udvikling inden for IT-sikkerhed ville være et fuldtidsarbejde i sig selv. Der er behov for en sparingspartner, der kommunikerer med jer på et niveau, som gør jer i stand til at træffe beslutninger ud fra deres ekspertviden.

FÅR DU DEN RETTE RÅDGIVNING TIL AT TRÆFFE DE RIGTIGE BESLUTNINGER?

8. SÆTTER I LIGHEDSTEGN MELLEM IT OG IT-SIKKERHED?

Cyberkriminalitet har nået et niveau og et omfang, hvor bekæmpelsen kræver specialistviden. Så man kan ikke længere regne med, at en dygtig IT-medarbejder eller IT-leverandør også kan tage sig af IT-sikkerhed på en optimal måde. IT er ikke det samme som IT-sikkerhed!

ER I OGSÅ KOMMET TIL DEN ERKENDELSE?

9. STILLER I KRAV TIL JERES IT-LEVERANDØR?

Hvis I er blandt dem, der outsourcer jeres IT, skal I være særligt opmærksomme på, om I også er dækket forsvarligt ind, hvad angår IT-sikkerhed. "Hele pakken er med" lyder selvfølgelig godt og nemt, men den snedige hacker får for let spil, hvis han ikke møder en værdig modstander.

HVAD GØR I FOR AT GARDERE JER?

10. HVORDAN KOMMER I VIDERE?

Hvis du har ubesvarede spørgsmål og vil i dialog med en erfaren samarbejdspartner, som ved, hvad der skal til for at komme hackeren i forkøbet, er du meget velkommen til at kontakte os hos IT Forum Gruppen.

Send en mail på kontakt@itf.dk eller ring på 70 100 150, så sørger vi for, at I bliver sat i kontakt med den rette rådgiver.

VI HJÆLPER JER MED DET RIGTIGE FORSVAR MOD CYBERANGREB.

KONTAKT OS

SIKKERHED FOR FREMDRIFT

Hos IT Forum Gruppen A/S sætter vi en ære i at forstå vores kunders drift, for kun sådan kan vi sikre de løsninger, der forhindrer nedbrud.

Vi ser ikke kun på virksomhedens udfordringer, men også på dens potentialer. Ved siden af den løbende kontakt i hverdagen, afholder vi statusmøder med det direkte formål at fordybe os i vores kunders behov og potentiale. Her byder vores specialister ind med forslag og løsninger, der understøtter virksomhedens kultur og krav.

Vi har blikket rettet mod fremtiden og de stadig nye trusler og muligheder indenfor IT. Samtidig er vi lokalt forankret med begge ben på jorden, mens vi stræber efter at skabe værdi i hver time, vi bruger.

IT Forum Gruppen A/S sikrer ikke alene den daglige drift. Vi udfordrer dig, så vi sikrer bedre udnyttelse af dine systemer, og vi inspirerer dig til at bruge nye løsninger. Kun sådan kan vi leve op til vores løfte.

Find flere tips til IT-sikkerhed her

70 100 150 :: KONTAKT@ITF.DK :: ITF.DK