Sikkerhedsaspekter

Din digitale arbejdsplads

Der florerer mange rædselshistorier om konsekvenserne af manglende sikkerhed omkring IT-løsninger, CPR-numre som sendes til Kina, hacking af Kørekortregisteret osv. Aviserne laver store overskifter, og alle taler om den nye Persondataforordning, og de mange udfordringer den vil give.

Overdrevet? – måske. Men på den anden side, så er der ingen røg uden ild. Så sikkerhed er noget, som skal tages særdeles alvorligt.

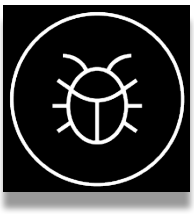
Langt de fleste sikkerhedsbrist kommer som en konsekvens af menneskelige fejl. Brugere er i langt de fleste tilfælde det svageste led i kæden.

Dette skyldes kun sjældent "ond vilje" eller bevidst sabotage. De hyppigste udfordringer kommer som en følge af uvidenhed, sjusk, manglende forståelse for de potentielle risici, gamle vaner, overbelastning eller tunge arbejdsgange. Og den typiske person, der skaber problemet, er blot en loyal medarbejder, som ønsker at være effektiv og gøre det bedste for virksomheden.

1 Udfordringerne

Udfordringerne dukker op under mange forskellige "hatte". Her er de seks vigtigste:

1.1 Ransomware



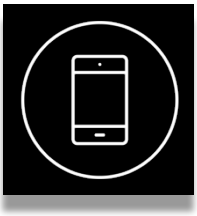
Ransomware viser sig, når der dukker en besked op, om at en Pc (eller server) er taget som "gidsel", at alle filer er krypteret, hvorefter det vil koster mange bitcoins få Pc'en og filerne gjort tilgængelig igen.

Udfordringen med Ransomware vokser og vokser. En af de bedst "indtjenende" angreb gav de kriminelle bagmænd mere end 3 millioner dollar.

Ransomware er på verdensplan mere indbringende end illegal narkotikahandel. Og det er meget nemt at sætte en "Ransomware-webshop" op.

Ransomware dukker op ad mange veje. Fordi systemer og PC'er ikke er opdateret med de seneste sikkerhedspatches; fordi der mangler et effektivt antivirus-system; fordi scanning af indkomne filer (og USB-nøgler) negligeres; eller fordi brugere uforvarende trykker på tilsyneladende uskyldige filer og links – eller de dukker op gennem indkomne e-mails.

1.2 Mobile brugere

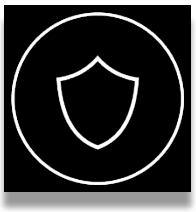


Dagens brugere er altid på farten. De skal have adgang til data og applikationer på alle tider af døgnet - hvad enten de er på arbejdet, der hjemme eller ude at rejse.

Forskellige brugere har forskellige behov og krav. Og en del af de enheder de bruger, er ikke virksomhedens med deres egne (BYOD – Bring Your Own Device). Og en gang i mellem bliver deres telefon/Pc forlagt – eller stjålet. Dette stiller krav til, at virksomhedsdata på mobile telefoner og tablets placeret i en såkaldt "container", hvor de ikke kan tilgås uden de rigtige rettigheder.

Dette rejser en lang række spørgsmål fra kontrol af identitet over sikre dataforbindelser til det at kunne finde, låse og slette enheden hvis den kommer i de forkerte hænder.

1.3 Administrative rettigheder



Hovedreglen er nem nok: Brugere skal ikke have administrative rettigheder til deres Pc - men så er der jo lige alle undtagelserne.

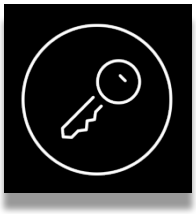
Der skal installeres programmer, som kræver, at den der installerer, er lokaladministrator. Og skal det gå stærkt, så er det nemmere at "låne" koden ud.

Så er der programmer, som kun kan afvikles som administrator.

Resultatet bliver ofte, at mange er lokal administrator, eller kender til password. Virksomheden taber overblikket, og alt for mange får adgang til data, de ikke skulle have adgang til.

En anden konsekvens er, at det bliver nemmere for ransomware og andre former for malware at inficere PC'en og derfra videre til data og backup.

1.4 Uautoriseret adgang

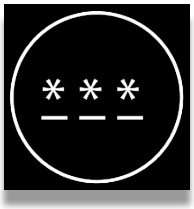


Der er andre former for malware end ransomware så som traditionel hacking eller phishing. Phishing er et internetfænomen, hvor en svindler forsøger at franarre godtroende internetbrugere deres brugernavn, adgangskode, kreditkort- eller netbankoplysninger.

Vejen ind er typisk e-mail eller internetsider.

Såvel hacking som phishing kan medføre tab af følsomme oplysninger - herunder persondata – hvilket kan påføre virksomheden store omkostninger, inklusive sanktioner fra det offentlige.

1.5 Password management

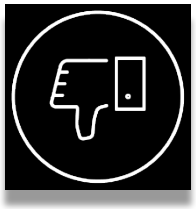


En engelsk undersøgelse har vist, at 30 % af alle sikkerhedsbrist hænger sammen med uforsvarlig omgang med kodeord, så som at dele disse med andre, anvende det samme "standard" kodeord, eller for svage regler omkring "styrken" i kodeord, og hvor ofte de skal deles.

Specielt deling af administratorkodeord kan være er en stor risiko.

En ubuden gæst som anvender et kendt brugernavn og et kendt kodeord, kan være meget vanskeligt at opdage eller standse.

1.6 Dårlig "offboarding"



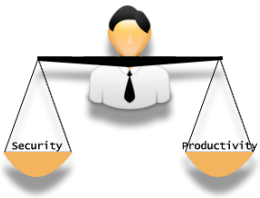
"Off-boarding" er processen, når en medarbejder holder op. Normal huskes nøgler, kreditkort og Pc/telefon.

Men hvad med data, der forsvinder ud på en USB-nøgle. Eller hvis det er en betroet IT-medarbejder? Hvad med alle de administratornavne og kodeord, som blev delt med alle de andre administratorer? – skiftes de?

Og hvad med adgang til data i skyen - og fra medarbejdere hos kunder og leverandører?

2 Hvad er så løsningen?

2.1 En afbalanceret strategi



Vores forslag er at skabe en balance mellem de to behov, der altid er i virksomheden – en balance mellem sikkerhed på den ene side og produktivitet på den anden side.

Ikke to virksomheder har samme behov for balance, men processen for at finde den er ens. Og Neisa kan hjælpe hele vejen igennem!

1. Det starter med de enkelte leders **individuelle erkendelse** af, at der eksisterer trusler og risici i dagens digitaliserede verden
2. Det skal følges op med en **kollektiv enighed** om, at sikkerhedsproblemerne er reelle og skal tages alvorligt
3. For hver potentielle risiko skal der skabes **risici-scenarier**: Hvad nu hvis?
4. For hvert scenarie skal der fastlægges et afbalanceret og realistisk **svar** – balance mellem risiko og produktivitet
5. Og så skal disse svar **implementeres og testes**