IT-SIKKERHEDSVURDERING

Februar 2022

VIRTULY

UDFORDRINGER OG RISICI

FUNDET UDFORDRINGER

6 ud af 8 forretningskritiske systemer har anmærkninger. 2 af dem er kritiske.

3 ud af 7 basale systemer har anmærkninger.

2 ud af 3 ukritiske systemer har anmærkninger.

1 ud af 4 persondatakilder har anmærkninger.

RISICI

Det er et markant øget antal hackerangreb fra især Rusland p.t.

63% af alle virksomheder under 500 medarbejdere, der udsættes for ransomware-angreb eksisterer ikke 6 måneder senere.

Omkostningen ved ransomware-angreb er opgjort til USD 133.000 i snit.

ANBEFALINGER

ANBEFALINGER

I prioriteret rækkefølge:

1. KRITISK: **Firewall** skal gøres utilgængelig via en offentlig URL.
2. På hver arbejdsstation skal browserens cache slettes for [redacted] dagligt.
3. På hver arbejdsstation skal der, som minimum, køres **Windows Update**, så basal sikkerhed er på plads.
4. Hjemmesidens Content Management System, **Wordpress**, og **plugins**, skal opdateres. De kan typisk sættes til at blive auto-opdateret.
5. To-faktorgodkendelse skal sættes op på **Dropbox** og **Microsoft Exchange Admin**.
6. Adgang for gamle medarbejdere skal fjernes i [redacted] **Dropbox** og **Office365**.
7. Systemlisten bør gennemgås og forventningerne til ejerne afstemmes internt.
8. Det kan overvejes at installere **Password Manager** på alle arbejdsstationer.
9. Få Virtuly til, hver måned, at udføre **Vulnerabilty, Penetration og User Awareness Testing** på virksomhedens vitale systemer og nøglemedarbejdere.

OMFANG

Virtuly har sammen med [redacted] indsamlet informationer om virksomhedens kernesystemer. Det giver et samlet øjebliksbillede af virksomhedens **opmærksomhed til sikkerhed** og **holdning til sikkerhed**.

Interviews: Der er gennemført interview med [redacted] for at opnå et indefra-ud syn på it-sikkerheden. Fokus er indefra-ud og centreret omkring a) systemejerskab, b) versionsopdateringer og c) rettighedskontrol på vigtigste systemer i organisationen.

Gray Box Testing: Der er testet for at opdage softwarefejl eller huller, hvor en vis begrænset viden om den underliggende software er kendt på forhånd. Denne form for "etisk hacking" giver mulighed for udefra-ind at se, hvor det er muligt at højne sikkerheden ved at lave rettelser og patches for at forhindre ondsindede angribere i at bruge disse udnyttelser.

IT-sikkerhedsvurderingen løser ikke anbefalingerne. [redacted] skal vurdere hvordan de bedst løses. Virtuly er behjælpelig med løsninger, såfremt dette ønskes.

HVAD VI HAR GJORT

KRITISKE FUND

SYSTEM	SÅRBARHEDS-VURDERING	FORRETNINGS-RISIKO	FUNDET
[redacted]	Stor	Høj	I systemet [redacted] På testede klientadgange var der cachede personfølsomme data, der strider mod GDPR. Gamle [redacted]-medarbejdere var ikke slettet fra systemadgang.
[redacted]	Lav	Mellem	Gamle [redacted]-medarbejdere var ikke slettet fra systemadgang.
Dropbox	Mellem	Mellem	To-faktorgodkendelse ikke aktiveret. Gamle [redacted]-medarbejdere var ikke slettet fra systemadgang.
E-conomic	Mellem	Mellem-høj	Den primære adgang er styret af en ekstern medarbejder.
Exchange	Lav-mellem	Lav	To-faktorgodkendelse ikke aktiveret.
Firewall	Stor	Høj	Firewall er tilgængelig fra en offentlig URL. Adgang til firewall udsætter i princippet al data og kontrol i virksomheden.
Harddisks	Mellem-høj	Mellem-høj	3 ud ca. 20 pc'ere testet for Windows Update. Ingen af dem var opdateret til seneste versioner. Det åbner for hackere at udnytte svagheder i gamle versioner af Windows.
Office365	Lav	Lav	Gamle [redacted]-medarbejdere var ikke slettet fra systemadgang.
[redacted]	Mellem	Mellem-høj	Ingen / usikkerhed om hvem, der ejer systemadministrationen på vegne af [redacted].
Password Manager	Mellem	Mellem	Der køres ikke med Password Manager. En Password Manager skaber unikke og stærke passwords.
Wordpress	Mellem	Mellem-høj	Wordpress og installerede plugins ikke er systemopdateret. Det åbner for hackere at udnytte svagheder i gamle versioner af Windows.

PERSONDATALÆK

TESTET	KOMPROMITTERINGER
[redacted]	E-mailinformation er blevet offentliggjort på et offentligt websted designet til at dele indhold.
[redacted]	E-mailinformation er blevet offentliggjort på et offentligt websted designet til at dele indhold.
[redacted]	123RF: Kompromitterede data: E-mailadresser, IP-adresser, navne, adgangskoder, telefonnumre, fysiske adresser, brugernavne. Appen: Kompromitterede data: e-mailadresser, arbejdsgivere, IP-adresser, navne, adgangskoder, telefonnumre. PDL-kunde: Kompromitterede data: e-mailadresser, arbejdsgivere, geografiske placeringer, jobtitler, navne, telefonnumre, profiler på sociale medier. GateHub: Kompromitterede data: E-mail-adresser, Krypterede nøgler, Mnemoniske sætninger, Adgangskoder. Onliner Spambot (spamliste): Kompromitterede data: E-mail-adresser, adgangskoder. Open Subtitles: Kompromitterede data: E-mail-adresser, geografiske placeringer, IP-adresser, adgangskoder, brugernavne. Verifications.io: Kompromitterede data: Fødselsdatoer, e-mailadresser, arbejdsgivere, køn, geografiske placeringer, IP-adresser, jobtitler, navne, telefonnumre, fysiske adresser
Tlf: [redacted]	Ingen kompromitteringer.

GENNEMGÅEDE SYSTEMER (1/2)

SYSTEM	EJER	VIGTIGHED	GENNEMGÅET	RISIKO
3G Modem	[redacted]	Lav-mellem	Tilgængelighed udefra	Adgang til [redacted] internet kan misbruges til ulovlige aktiviteter [redacted]
[redacted]	[redacted]	Høj	Rettighedskontrol Gamle brugere Gamle kampagner Personfølsomme data	[redacted] personfølsomme data fx kan tilgåes fordi browseren ikke rydder cachen, vil det være et brud på GDPR, der kan medføre bødestraf. Unødig adgang til udveksling af data mellem [redacted] og kunderne kan i værste fald medføre datalæk.
[redacted]	[redacted]	Mellem-høj	To-faktorgodkendelse Rettighedskontrol Phishing	Unødig adgang til banken giver unødig indsigt i virksomhedens finansielle aktiviteter og i værste fald kan der ske uberettigede betalinger.
Backup	[redacted]	Mellem	Der køres ikke med backup, da kernesystemer er tredjeparts-cloudservices.	Vigtigt at ingen kritiske data gemmes på lokale harddiske.
[redacted]	[redacted]	Mellem	Rettighedskontrol Gamle brugere Gamle kampagner Personfølsomme data	[redacted] personfølsomme data fx kan tilgåes fordi browseren ikke rydder cachen, vil det være et brud på GDPR, der kan medføre bødestraf. Unødig adgang til udveksling af data mellem [redacted] og kunderne kan i værste fald medføre datalæk.
Datto	[redacted]	Mellem	Rettighedskontrol Gamle brugere	Unødig adgang til udveksling af data mellem [redacted] og kunden kan i værste fald medføre datalæk.
Domæne	[redacted]	Lav	Sikre https Tjekke phishing-forsøg Rettighedskontrol	Et domæne, der ikke kører https er mere udsat for at blive hacket. Phishing-forsøg vil lede kunder til andre sider, der misbruger [redacted] troværdighed.
Dropbox	[redacted]	Mellem	To-faktorgodkendelse Version på lokal maskine Gamle brugere Rettighedskontrol Adgang til data	Gamle eller falske brugere kan få adgang til forretningskritiske og personfølsomme data.
e-conomic	[redacted]	Mellem-høj	To-faktorgodkendelse Gamle brugere	Unødig adgang til regnskabssystemet giver unødig indsigt i virksomhedens finansielle aktiviteter og kunder.

GENNEMGÅEDE SYSTEMER (2/2)

SYSTEM	EJER	VIGTIGHED	GENNEMGÅET	SYSTEMRISICI
Exchange	[redacted]	Lav	To-faktorgodkendelse Gamle brugere Domænerettigheder	Gamle eller falske brugere kan få adgang til firewalls, routere, domæner, filer og systemer. Adgangen kan også misbruges på eksterne sider og tjenester.
Firewall	[redacted]	Høj	To-faktorgodkendelse Rettighedskontrol Tilgængelighed udefra	Hvis firewallen ikke er systemopdateret og beskyttet, er den mere udsat for at blive hacket. Al data er i princippet tilgængeligt for hackeren. Gendannelse af netværket vil i værste fald være helt fra bunden af.
[redacted]	[redacted]	Mellem-høj	Rettighedskontrol Gamle brugere	[redacted] og kunderne, er brud på GDPR, der kan medføre bødestraf. Unødig adgang til udveksling af data mellem kunden og kundens kan i værste fald medføre datalæk.
Harddisk	[redacted]	Mellem	Firewall Styresystemsversion Filer på lokale drev Personfølsomme data	Hvis en pc ikke er styresystemsopdateret og beskyttet, er den mere udsat for at blive hacket. Data gemt lokalt vil være udsat. Gendannelse af tabt data er stort umuligt.
Netværksrouter	[redacted]	Høj	To-faktorgodkendelse Rettighedskontrol Tilgængelighed udefra	Hvis netværksrouteren ikke er systemopdateret og beskyttet, er den mere udsat for at blive hacket. Al data er i princippet tilgængeligt for hackeren. Gendannelse af netværket vil i værste fald være helt fra bunden af.
Office365	[redacted]	Lav	To-faktorgodkendelse Gamle brugere Unødige licenser	Gamle eller falske brugere kan få adgang til forretningskritiske og personfølsomme data. Adgangen kan også misbruges på eksterne sider og tjenester.
[redacted]	-	Mellem-høj	Rettighedskontrol Gamle brugere Gamle kampagner Personfølsomme data	[redacted] personfølsomme data fx kan tilgåes fordi browseren ikke rydder cachen, vil det være et brud på GDPR, der kan medføre bødestraf. Unødig adgang til udveksling af data mellem[redacted] og kunderne kan i værste fald medføre datalæk.
Password Manager	[redacted]	Mellem	*Der køres ikke med Password Manager.*	De fleste mennesker har en tendens til at bruge de samme 4-5 passwords. Det betyder, at lækkes en email-adresse og et password kan den kombination testes på tusindvis af services. En Password Manager skaber unikke og stærke passwords.
Wordpress	[redacted]	Mellem-høj	Systemversion Gamle brugere Plugins Malware	Hvis Wordpress og installerede plugins ikke er systemopdateret og beskyttet, er den mere udsat for at blive hacket. Gendannelse af hjemmeside er i værste fald helt fra bunden af.

SUND FORNUFT

IT-OPMÆRKSOMHED

De fleste it-problemer kan løses via sund fornuft.

Når vi taler om it-opmærksomhed handler det om at huske ”at lukke døre og vinduer i huset” og ikke reagere på mistænkelige henvendelser og forespørgsler.

IT-HOLDNING

It-holdning handler om de grundprincipper virksomheden har til it.

Det vil typisk være at alle systemer har en ansvarlig, der sørger for at systemet er opdateret, ingen uvedkommende har adgang og adgangen dertil afspejler risikoen.

Det handler også om at have en Plan B, hvis noget går galt.

TAK FOR OPMÆRKSOMHEDEN!

BRUG FOR MERE HJÆLP TIL IT-SIKKERHED?

KONTAKT: HENRIK WORSØE | HEJ@VIRTULY.DK | +45 3242 2878

VIRTULY