Risikoområde	Risiko - hvad kan påvirke fortrolighed, tilgængelighed eller integritet?	Risikoejer
Enheder	Manglende forsvar mod malware	
Enheder	Ukendte enheder i virksomheden	
Netværk	Manglende kontrol over netværksadgang til enheder	
Vurdér egne applikationer	Bogføringssystem bliver kompromitteret	
Vurdér egne applikationer	CRM: CRM-system bliver kompromitteret	
Vurdér egne applikationer	Dokumenthåndteringssystem (ESDH): Dokumenthåndteringssystem (ESDH) bliver kompromitteret	
Vurdér egne applikationer	E-mail: E-mail-system bliver kompromitteret	
Vurdér egne applikationer	Filserver: Filserver bliver kompromitteret	
Vurdér egne applikationer	Hjemmeside (CMS): Hjemmeside (CMS) bliver kompromitteret	
Vurdér egne applikationer	Kontorplatform (Fx O365/Google): Kontorplatform bliver kompromitteret	
Vurdér egne applikationer	Projektstyring: Projektstyringssystem bliver kompromitteret	
Vurdér egne applikationer	Tidsregistrering: Tidsregistreringssystem bliver kompromitteret	

Vurdér egne applikationer	Vagtplanlægning: Vagtplanlægningssystem bliver kompromitteret
Applikationer og tjenester	Manglende overblik over jeres applikaitoner og tjenester
Brugere	Uopmærksomme brugere
Brugere	Uønsket adgang via inaktive brugere
Netværk	Manglende overblik over jeres netværk
Netværk	Uønsket aktivitet på netværket
Brugere	Manglende kontrol med brugerrettigheder
Data	Datatab
Netværk	Uopdateret netværk
Data	Unødvendig adgang til data

Styring	IT-sikkerhedsstyring

Risikovurdering

Hvorfor er dette en risiko?	Indtastet sandsynlighed (1-5)	Hvorfor vurderes sandsynligheden til dette?
Enheder som ikke har antivirus eller ikke er opdaterede er særligt sårbare over for malware.	1	Fordi alle enheder i virksomheden har antivirus, som holdes opdateret
Ukendte enheder (f.eks. IoT-produkter, printere eller smartphones) tilkoblet virksomhedens netværk kan være en usikker indgang til virksomheden eller være skadelige i sig selv.	2	Fordi medarbejderne kan tage egne smartphones med på arbejde
Port-skanning kan bruges af hackere til at finde åbne og aktive porte, hvor de nemt kan få adgang til services, der kan angribes.	2	Fordi åbne porte ikke kontrolleres ud over installation og setup af firewall på de enkelte enheder
Systemer og applikationer som ikke opdateres og ikke overvåges kan fungere som sikkerhedshul.	1	Fordi bogføringssystem kommer udefra med en serviceaftale
Systemer og applikationer som ikke opdateres og ikke overvåges kan fungere som sikkerhedshul.	1	Fordi CRM-system kommer udefra med en serviceaftale
Systemer og applikationer som ikke opdateres og ikke overvåges kan fungere som sikkerhedshul.	1	Fordi dokumenthåndteringssystem kommer udefra med en service-aftale
Systemer og applikationer som ikke opdateres og ikke overvåges kan fungere som sikkerhedshul.	1	Fordi E-mail-system kommer udefra med en serviceaftale
Systemer og applikationer som ikke opdateres og ikke overvåges kan fungere som sikkerhedshul.	1	Fordi filserveren godt nok er in-house, men den holdes opdateret og så sikker som mulig
Systemer og applikationer som ikke opdateres og ikke overvåges kan fungere som sikkerhedshul.	1	Fordi hjemmesiden hostes udefra med en serviceaftale
Systemer og applikationer som ikke opdateres og ikke overvåges kan fungere som sikkerhedshul.	1	Fordi platformen kommer udefra med en serviceaftale
Systemer og applikationer som ikke opdateres og ikke overvåges kan fungere som sikkerhedshul.	1	Fordi systemet kommer udefra med en serviceaftale
Systemer og applikationer som ikke opdateres og ikke overvåges kan fungere som sikkerhedshul.	1	De har ikke faste mødetider

Systemer og applikationer som ikke opdateres og ikke overvåges kan fungere som sikkerhedshul.	1	De har ikke faste mødetider
Et manglende overblik over accepterede og installerede applikationer kan resultere i ondsindet eller uopdateret software på enheder og netværk.	3	Fordi medarbejderne kan frit installere ny software, men er selv ret opmærksomme på IT-sikkerhed
Hackerne tiltvinger sig adgang ved at lokke brugerne til at hente og åbne ondsindet malware via deres webbrowsere eller via links i e-mails.	3	Fordi medarbejderne er godt klar over, at man ikke må åbne tilfældige links.
Inaktive brugerkonti, særligt dem med administratorrettigheder, kan misbruges til at skaffe sig utilsigtet adgang til virksomheden og til at slette backup.	1	Der er ikke nogle inaktive admin-brugere på nuværende tidspunkt
Uden en oversigt er det vanskeligt at identificere trafikken og tilrette konfigurationen af netværket, hvilket gør netværket sårbart over for hackere og malware.	3	Fordi der ikke skabes et helt overblik over netværket
Ondsindet netværksaktivitet kan foregå uopdaget uden aktiv logning. Og ved manglende netværkssegmentering kan aktiviteten foregå på tværs af netværket.	3	Fordi der måske benyttes SIEM, men nok ikke tilstrækkelig segmentering
Udefrakommende og medarbejderes unødige adgang til en administratorkonto kan udnyttes ved at tildele loginet privilegier og skabe rutiner, der bliver ved med at skabe huller i virksomhedens IT-systemer eller til at slette data og/eller backups.	2	Der er opdeling af rettigheder mellem de forskellige brugere og typer af brugere
Kan medføre uerstattelige tab, skade omdømme, medføre sagsanlæg/bødestraf og umuliggøre driften.	2	Fordi der foretages backups. De testes uregelmæssigt
Det er ofte via forældede versioner af netværksenhedernes software (routere, firewalls, DNS-servere, DHCP-servere etc.), at hackere tvinger sig adgang til netværket.	3	Fordi opdateringer ikke foretages, men diverse indstillinger er dog tilpasset virksomheden og standard kodeord er ændret
Brugere med unødig adgang til data kan misbruge denne til at skade virksomheden.	1	Fordi der er et månedligt tjek, der fjerner rettigheder fra alle og derefter tildeles de igen efter behov

Manglende overblik og strying af IT-sikkerheden	3	Medium kontrol

Indtastet konsekvens (1-5)	Hvorfor vurderes konsekvensen til dette?	Beregnet risiko	Acceptert (ja/nej)	Nye foranstaltninger
3	Den enkelte enhed er ikke så vigtig. Det er muligheden for propagering dog	3	Ja	
2	Medfører til ikke at have fuld oversigt over netværket. Desuden er der ingen garanti for, der ikke er noget ondsindet på enhederne	4	Accepteres	
2	Det er begrænset, hvor meget der hostes selv. Det kan derfor være mindre relevant	4	Undgå	Sørg for god opsætning af firewalls
1	Virksomheden kan i princippet godt fortsætte med et sådan sikkerhedshul	1	Accepteres	
2	Virksomheden kan i princippet godt fortsætte med et sådan sikkerhedshul	2	Accepteres	
3	Virksomheden kan i princippet godt fortsætte med et sådan sikkerhedshul	3	Accepteres	
2	Virksomheden kan i princippet godt fortsætte med et sådan sikkerhedshul	2	Accepteres	
5	Hvis kode og andet ikke kan tilgås vil det fastfryse virksomheden i tiden	5	Accepteres	
5	Hjemmesiden er virksomhedens produkt	5	Accepteres	
2	Virksomheden kan i princippet godt fortsætte med et sådan sikkerhedshul	2	Accepteres	
4	Det kan være svært at udvikle videre på virksomhedens produkt, hvilket kan skabe problemer på den lange bane	4	Accepteres	
1		1	Accepteres	

1		1	Acceptere s	
3	Det kan føre til malwareangreb	9	Overvåges	Lav whitelist
3	Det skaber en mulig åbning for hackere/malware	9	Undgå	Indfør obligatorisk træning af medarbejderne på jævn basis
5	Intregitet af data kan kompromitteres	5	Overvåges	Der skal månedligt være et tjek, der fratager alle brugere alle rettigheder og tildeler dem igen efter behov
3	Fordi det kan skabe en åbning for hackere	9	Overvåges	Skab totalt overblik
3	Det er begrænset, hvor meget der hostes selv	9	Overvåges	Sørg for fuld implementering af SIEM
5	Intregitet af data kan kompromitteres	10	Undgå	Der skal månedligt være et tjek, der fratager alle brugere alle rettigheder og tildeler dem igen efter behov
5	Virksomheden lever af data. Uden sin data, kan virksomheden ikke fortsætte sit virke	10	Forsikring	Fortsæt med at tage backups, men sørg for også at teste, at man kan lave fuld recovery fra disse regelmæssigt
4	Åbner mulighed for, at hackere kan komme ind på netværket	12	Undgå	Sørg for jævn opdatering af enheder
5	Mulig komprommittering af data	5	Acceptere s	

4	Muligt problem	12	Undgå	IT-sikkerhedsstyring

Risikohåndtering

Ny sandsynlighed (1-5)	Konsekvens efter nye foranstaltninger (1-5)	Ny restrisiko	Restrisiko Acceptere t	Konklusion
		0		
		0		
1	2	2	Acceptere s	
		0		
		0		
		0		
		0		
		0		
		0		
		0		
		0		
		0		
		0		

		0	
1	3	3	Acceptere s
2	3	6	Forsikring
1	5	5	Acceptere s
1	3	3	Acceptere s
1	3	3	Acceptere s
1	5	5	Acceptere s
1	5	5	Acceptere s
1	4	4	Acceptere s
		0	

1	2	2	Acceptere s

Kilder til håndtering

https://sikkerdigital.dk/virksomhed/hvad-truer-din-virksomhed/virus-og-malware/

https://www.cfcs.dk/da/forebyggelse/vejledninger/cyberforsvar-der-virker/

https://cfcs.dk/globalassets/cfcs/dokumenter/rapporter/CFCS-rapport-anatomien-af-ma

https://sikkerdigital.dk/virksomhed/syv-raad-om-it-sikkerhed/2-opdater-programmer-lo

https://sikkerdigital.dk/virksomhed/syv-raad-om-it-sikkerhed/2-opdater-programmer-lo

https://sikkerdigital.dk/virksomhed/syv-raad-om-it-sikkerhed/2-opdater-programmer-lo

https://sikkerdigital.dk/virksomhed/syv-raad-om-it-sikkerhed/2-opdater-programmer-lo

https://sikkerdigital.dk/virksomhed/syv-raad-om-it-sikkerhed/2-opdater-programmer-lo

https://www.sikkerdigital.dk/virksomhed/syv-raad-om-it-sikkerhed/2-opdater-programn

https://www.sikkerdigital.dk/virksomhed/syv-raad-om-it-sikkerhed/2-opdater-programn

https://sikkerdigital.dk/virksomhed/syv-raad-om-it-sikkerhed/2-opdater-programmer-lo

https://www.sikkerdigital.dk/virksomhed/syv-raad-om-it-sikkerhed/2-opdater-programn

https://www.sikkerdigital.dk/virksomhed/syv-raad-om-it-sikkerhed/2-opdater-programn

https://sikkerdigital.dk/virksomhed/syv-raad-om-it-sikkerhed/1-faa-overblik-over-vigtige

https://www.sikkerdigital.dk/virksomhed/leder/medarbejderpakken

https://www.sikkerdigital.dk/virksomhed/it-sikkerhedsansvarlig/styring-af-adgangsrettig

https://www.cfcs.dk/da/forebyggelse/vejledninger/cyberforsvar-der-virker/

https://www.cfcs.dk/da/forebyggelse/vejledninger/logning/

https://www.sikkerdigital.dk/virksomhed/it-sikkerhedsansvarlig/styring-af-adgangsrettig

https://sikkerdigital.dk/virksomhed/syv-raad-om-it-sikkerhed/4-tag-backup-af-data/

https://cfcs.dk/globalassets/cfcs/dokumenter/rapporter/-undersoegelsesrapport-kompr

https://www.sikkerdigital.dk/virksomhed/it-sikkerhedsansvarlig/styring-af-adgangsrettig

CIS kontroller til håndtering af risiko

Relevante CIS-kontroller mht. antimalware:
8.1 Utilize Centrally Managed Anti-Malware Software
8.4 Configure Anti-Malware Scanning of Removable Media
8.5 Configure Devices to Not Auto-Run Content

Relevante CIS-kontroller mht. ukendte enheder:
1.4 Maintain Detailed Asset Inventory
1.6 Address Unauthorized Assets

Relevant CIS-kontrol mht. port-skanning:
9.4 Apply Host-Based Firewalls or Port-Filtering

Relevante CIS-kontroller mht. eget system:
3.4 Deploy Automated Operating System Patch Management Tools
3.5 Deploy Automated Software Patch Management Tools

Relevante CIS-kontroller mht. eget system:
3.4 Deploy Automated Operating System Patch Management Tools
3.5 Deploy Automated Software Patch Management Tools

Relevante CIS-kontroller mht. eget system:
3.4 Deploy Automated Operating System Patch Management Tools
3.5 Deploy Automated Software Patch Management Tools

Relevante CIS-kontroller mht. eget system:
3.4 Deploy Automated Operating System Patch Management Tools
3.5 Deploy Automated Software Patch Management Tools

Relevante CIS-kontroller mht. eget system:
3.4 Deploy Automated Operating System Patch Management Tools
3.5 Deploy Automated Software Patch Management Tools

Relevante CIS-kontroller mht. eget system:
3.4 Deploy Automated Operating System Patch Management Tools
3.5 Deploy Automated Software Patch Management Tools

Relevante CIS-kontroller mht. eget system:
3.4 Deploy Automated Operating System Patch Management Tools
3.5 Deploy Automated Software Patch Management Tools

Relevante CIS-kontroller mht. eget system:
3.4 Deploy Automated Operating System Patch Management Tools
3.5 Deploy Automated Software Patch Management Tools

Relevante CIS-kontroller mht. eget system:
3.4 Deploy Automated Operating System Patch Management Tools
3.5 Deploy Automated Software Patch Management Tools

Relevante CIS-kontroller mht. eget system:
3.4 Deploy Automated Operating System Patch Management Tools
3.5 Deploy Automated Software Patch Management Tools

Relevante CIS-kontroller mht. eget system:
3.4 Deploy Automated Operating System Patch Management Tools
3.5 Deploy Automated Software Patch Management Tools

Relevante CIS-kontroller mht. systemoverblik:
2.1 Maintain Inventory of Authorized Software
2.2 Ensure Software Is Supported by Vendor
2.6 Address Unapproved Software

Relevante CIS-kontroller mht. uopmærksomme brugere:
17.3 Implement a security awareness program
17.4 Update awareness content frequently
17.5 Train workforce on secure authentication
17.6-17.9

Relevante CIS-kontroller mht. inaktive brugere:
16.8 Disable Any Unassociated Accounts
16.9 Disable Dormant Accounts
16.11 Lock Workstation Sessions After Inactivity

Relevante CIS-kontroller mht. netværksoversigt:
12.1 Maintain an Inventory of Network Boundaries
12.4 Deny Communication Over Unauthorized Ports

Relevante CIS-kontroller mht. aktiv logning og netværkssegmentering:
6.2 Activate Audit Logging
15.7 Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data
15.10 Create Separate Wireless Network for Personal and Untrusted Devices
12.1 Maintain an Inventory of Network Boundaries
12.6 Deploy Network-Based IDS Sensors
12.7 Deploy Network-Based Intrusion Prevention Systems
12.8 Enable the collection of NetFlow and logging data on all network boundary devices.

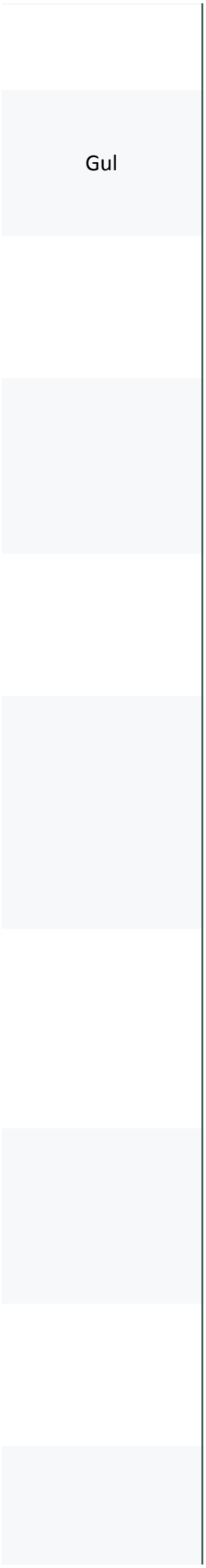
Relevante CIS-kontroller mht. administratorrettigheder:
4.2 Change Default Passwords
4.3 Ensure the Use of Dedicated Administrative Accounts

Relevante CIS-kontroller mht. gendannelse af data:
10.1 Ensure Regular Automated Backups
10.2 Perform Complete System Backups
10.4 Protect Backups
10.5 Ensure All Backups Have at Least One Offline Backup Destination

Relevant CIS-kontrol mht. netværksopdateringer:
11.4 Install the Latest Stable Version of Any Security-Related Updates on All Network Devices

Relevant CIS-kontrol mht. adgang til data:
14.6 Protect Information Through Access Control Lists
13.1 Maintain an Inventory of Sensitive Information
13.2 Remove Sensive Data or Systems Not Regularly Accessed by Organization

Risikovillighed
Grøn
1
6
Rød
10


Gul