Du kan med fordel overlade din IT-sikkerhed til os

IT-sikkerhed er blevet mere komplekst og kræver anvendelse af ekspertviden og den rigtige teknologi. Hos IT Relation vurderer vi løbende hvilke standarder, teknikker og værktøjer, der giver din virksomhed den mest optimale beskyttelse.

ITRelation®
HVERDAGENS IT SUPERHELTE

Sikkerhedspakker

Fremfor kun at tilbyde enkeltstående sikkerhedsprodukter, har vi udviklet tre sikkerhedspakker, der bygger på en helhedsorienteret sikkerhedsmodel med løbende vurdering og opfølgning som vist i nedenstående figur.

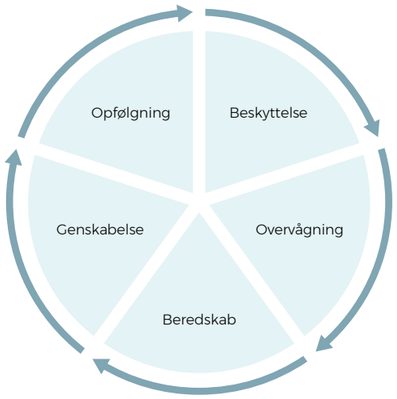
Pakkerne indeholder udvalgte sikkerhedsprodukter i samspil med en fælles "berigelse" i form af ekstra services. Pakkerne kan udvides med optioner, der dækker specifikke forhold i jeres organisation.

Pakkernes indhold revideres løbende og kan dermed variere over tid, afhængigt af faciliteter, kvalitet og pris. Vi understøtter produkterne i en periode efter de udgår af nysalg, så længe det teknisk og økonomisk giver mening. Når det er relevant at udskifte elementer, tager vi kontakt til jer og aftaler det nærmere forløb.

Pakkerne er delt ind i grupperne klientsikkerhed, serversikkerhed og fortrolighed. Til hver gruppe tilbydes en pakke til "basic" sikkerhedsbehov og en pakke til "high" sikkerhedsbehov. Vores konsulenter vil hjælpe med at afdække jeres behov i forhold til denne inddeling og yder rådgivning med hensyn til tilkøb af ekstra ydelser.

De følgende sider beskriver formål og hvilken ydelse, der leveres i forbindelse med de enkelte elementer i pakkerne. De forskellige produkter beskrives primært ud fra en IT-sikkerhedsvinkel, men indeholder også mange funktioner, der generelt gør det lettere at administrere jeres IT-miljø.

Pakkernes pris kalkuleres samlet ud fra parametre som antal brugere, antal devices og frekvens af scanninger og reviews.



Klientsikkerhed

Klientsikkerhedspakken understøtter IT-sikkerheden knyttet til udstyr og netværk, der anvendes af slutbrugere.
Indholdet i pakken er grupperet efter de forskellige faser i vores sikkerhedsmodel.

Få en uddybende forklaring på produkterne/ydelserne på side 12.

Klientsikkerhedspakke

PRODUKT/YDELSE	BASIC	HIGH
Beskyttelse		
Antivirus/malware-beskyttelse	✓	✓
Virus/spam scanning af e-mails	✓	✓
Patch management	✓	✓
DNS-filtrering	✓	✓
Device Management		✓
Port Security		✓
Awareness nyheder		✓
OPTION: Mobile device management (MDM)		
Overvågning		
Overvågning	✓	✓
OPTION: Eskalering		
OPTION: Intrusion detection/prevention på lokalnet		
Beredskab		
Sikkerhedshotline	✓	✓
Beredskab til geninstallation		✓
Genskabelse		
Geninstallation af angrebne klienter (laptops, PC'er o.lign.)		✓
Opfølgning		
Ekstra review		✓
Regelmæssige aktiviteter		
Review med aftalte intervaller		✓
OPTION: Awarenes test		
OPTION: Fishing test		

Serversikkerhed

Denne pakke dækker IT-sikkerheden knyttet til jeres servere med jeres specifikke applikationer og data.
Indholdet i pakken er grupperet efter de forskellige faser i vores sikkerhedsmodel.

Få en uddybende forklaring på produkterne/ydelserne på side 14.

Serversikkerhedspakke

PRODUKT/YDELSE	BASIC	HIGH
Beskyttelse		
Antivirus/malware-beskyttelse	✓	✓
Patch management		✓
Firewall	✓	✓
Advanced malware protection		✓
Multifaktor autentificering	✓	✓
Reset password		✓
DNS-filtrering	✓	✓
Overvågning		
Overvågning	✓	✓
Eskalering		✓
OPTION: Intrusion detection/prevention i servernetværk		
Beredskab		
Sikkerhedshotline	✓	✓
Beredskab til geninstallation		✓
Genskabelse		
Geninstallation af angrebne servere		✓
Opfølgning		
Ekstra review		✓
Regelmæssige aktiviteter		
Regelmæssig sårbarhedsscanning	✓	✓
Review med aftalte intervaller		✓
Audit		✓
Test af genetablering		✓

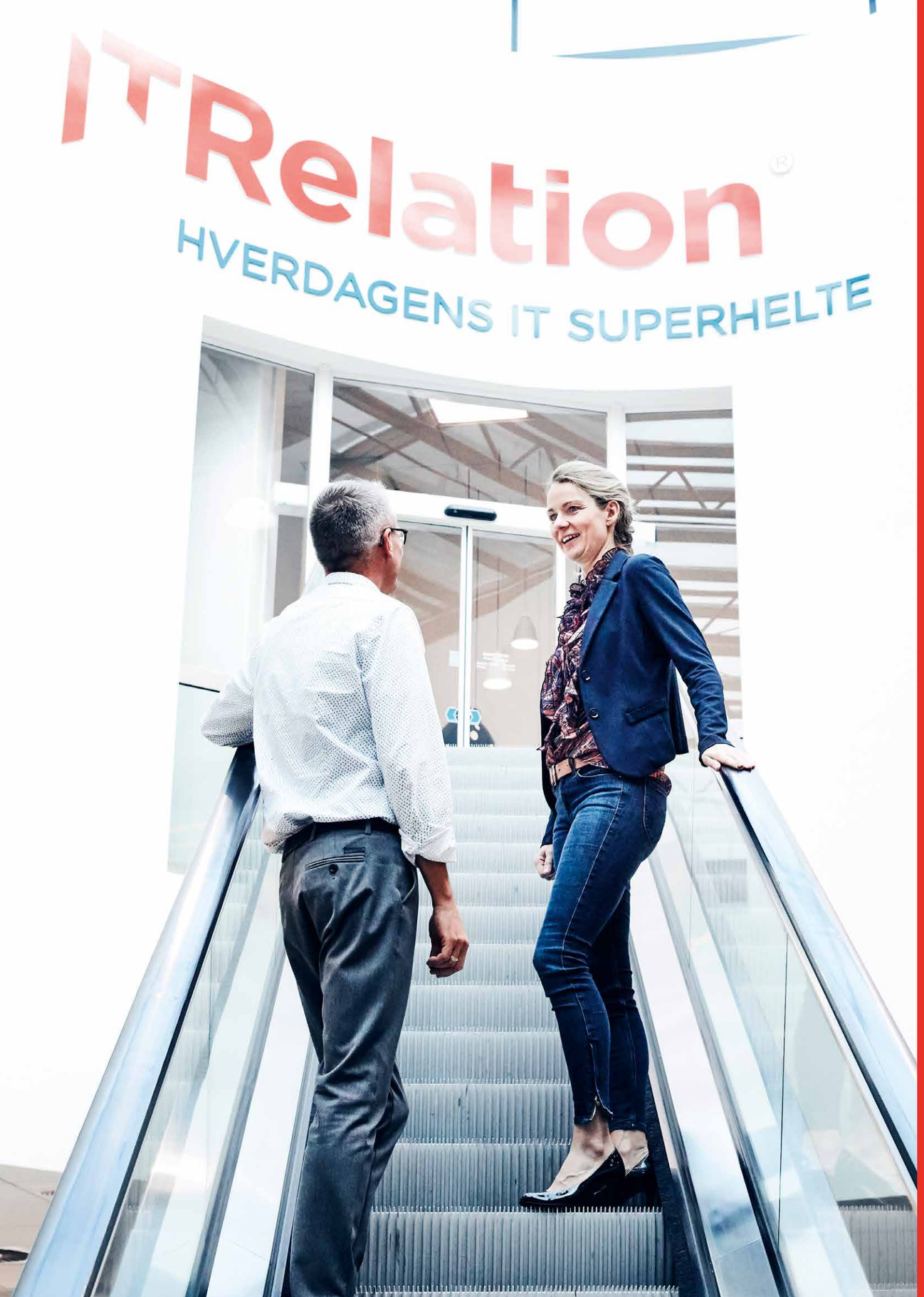
Fortrolighed

Denne pakke dækker specifikt IT-sikkerheden knyttet til jeres fortrolige data. Disse produkter og services bygger på en høj grad af sikkerhed på klient og serversiden, og skal derfor ses som udvidelser til de øvrige pakker.
Indholdet i pakken er grupperet efter de forskellige faser i vores sikkerhedsmodel.

Få en uddybende forklaring på produkterne/ydelserne på side 16.

Fortrolighedspakke

PRODUKT/YDELSE	BASIC	HIGH
Beskyttelse		
Løbende uddannelse af medarbejder privacy awareness	✓	✓
Sikker mail med tunnelkryptering og Send Sikkert Outlook plugin		✓
Data leak/loss prevention “light”		✓
Virtuelt Privat Netværk - VPN	✓	✓
OPTION: Digital signering		
OPTION: Password Management		
Overvågning		
Overvågning af sikker mail løsningen		✓
Eskalering		✓
Beredskab		
Sikkerhedshotline	✓	✓
Beredskab til analyse af mail-flow		✓
Genskabelse		
Manuel gensendelse af sikre mails		✓
Opfølgning		
Ekstra review		✓
Regelmæssige aktiviteter		
Review med aftalte intervaller		✓
Audit		✓
OPTION: Data Discovery		



Få det uddybet

Få en uddybende beskrivelse af, hvad de forskellige produkter/ydelser dækker over i de respektive sikkerhedspakker. Forklaringen er delt ind i samme rækkefølge, som du finder i tabellen.

Klientsikkerhed

Beskyttelse

Antivirus/malware-beskyttelse
Antivirus/malwarebeskyttelse beskytter generelt mod uautoriserede-de programmer (orme, trojanske heste, adware, spyware mm.), der kan genere eller forsage skade. Beskyttelsen baserer sig bl.a. på online malware-databaser, der løbende opdateres.
Malwarebeskyttelses-programmet installeres direkte på jeres PC'er, laptops, smartphones, mm. og kan overvåges centralt.

Virus/spam scanning af e-mails
E-mails er ofte den letteste kanal til spredning af uautoriserede programmer enten direkte eller via links. Scanningen beskytter også mod såkaldte fishing mails og CFO fraud, dvs. mails der lokker brugere til at opgive fortrolige oplysninger, overføre penge eller lignende.
Scanningen installeres som en del af mail-flowet mellem jeres mailserver og internettet.

Patch Management
Al software indeholder sårbarheder eller fejl i større eller mindre grad. Det er derfor vigtigt altid at være fuldt opdateret, så man får gavn af vigtige rettelser, der ellers kan udnyttes af IT-kriminelle. Det er et stort arbejde at holde alt opdateret, og Patch Management værktøjerne gør det lettere, idet det kan håndtere de fleste almindelige programmer automatisk, opdatere på passende tidspunkter og i mange tilfælde mens programmerne kører og uden at genstarte. Servicen inkluderer ikke deciderede opgraderinger af software.
Patch Management installeres direkte på jeres PC'er, laptops, mm. og styres centralt.

DNS-filtrering
Mange angreb starter med, at brugeren klikker på et link i en e-mail eller på en hjemmeside. DNS-filtrering sikrer, at man ikke kan komme ind på de sider, der allerede er kendt for at indeholde malware. Databaserne opdateres kort efter opdagelse af nye trusler. Servicen kan overvåges og styres centralt.
DNS-filtrering etableres ved en simpel opsætning på laptops mm. og trækker på en fælles service med den opdaterede database over malware hjemmesider.

Device Management
Jo bedre I kender det udstyr (devices), der kobles på jeres netværk, jo lettere kan I skabe overblik over trusler og sårbarheder. Med Device Management kan man både overvåge hvilke devices, der er koblet på, og man kan styre, hvad de enkelte devices har adgang til og evt. helt afskære dem fra adgang, hvis de er angrebet, eller brugeren har forladt virksomheden, fået sit udstyr stjålet eller lignende.
Device Management består dels af programmer, der installeres på de enkelte devices, og dels af et centralt kontrolprogram.

Port security
I mange tilfælde er det nemt at koble udstyr i det lokale netværk – det er blot et stik i væggen eller en tilslutning via trådløst netværk. Det giver dels en let adgang til at tilslutte udstyr, der ikke er sikkerhedsgodkendt, f.eks private PC'er, smartphones o.lign., eller for uvedkommende til at overvåge netværkstrafik og angribe andet udstyr.
Med port security skal alt udstyr godkendes for at kunne tilsluttes. Port security etableres via protokollen 802.1x i jeres eksisterende netværks udstyr.

Awareness nyheder
Angreb optræder ofte i bølger med ensartede teknikker. Med Awareness nyheder vil vi periodisk informere om særlige forholdsregler jeres brugere skal iagttage. Indholdet vil have fokus på en anbefalet adfærd frem for detaljerede tekniske forklaringer.

OPTION: **Mobile device management (MDM)**
Smartphones og tablets anvendes i dag i mange tilfælde på lige fod med PC'er og laptops. MDM giver mulighed for centralt at styre hvilke devices, der har adgang og hvilke applikationer de må benytte og derigennem er med til at sikre overholdelse af jeres virksomheds IT-sikkerhedspolitikker.

Overvågning

De beskyttelsesprodukter vi anvender indeholder i dag næsten alle et kontrolværktøj. Ved at vi overvåger alle produkterne samlet, kan vi opdage angreb og uhensigtsmæssigheder så tidligt som muligt.
Dette er en væsentlig fordel i at samle produkterne i en pakke, idet en overvågning af produkterne enkeltvis ikke giver det fulde billede.

Overvågning
Overvågningen, der er delvist automatisk og delvist manuel, kan f.eks. afdække, at bestemte PC'er eller brugere er særligt udsatte.
Hvis vi opdager alvorlige problemer, vil vi følge op og løse dem i fællesskab med jer.
Der kan yderligere installeres et "cloud malware protection" program på jeres udstyr, der sikrer, at data om installeret software mm. indgår i overvågningen, og det kan bl.a. vise, hvilket udstyr, der er angrebet, hvis det først senere viser sig at være ondsindet software. Oplysningerne kan også anvendes i de regelmæssige reviews. Overvågningen dækker alle de beskyttelsesprodukter, der er indeholdt i pakken.

OPTION: **Eskalering**
Hvis der i forbindelse med overvågningen opdages kritiske sårbarheder behandles og eskaleres de på linje med driftsafbrydelser o.lign. Dvs. vi tager kontakt til jer og sammen vurderer truslen og evt. aktiviteter til imødegåelse.

OPTION: **Intrusion detection/ prevention på lokalnet**
Udstyr placeret i netværket, der overvåger netværkstrafikken kan detektere tegn på indbrud i netværket, som er kommet gennem den øvrige beskyttelse og ikke er opdaget af den øvrige overvågning. Udstyret kan dels give alarm og dels stoppe eller begrænse angrebet i mange tilfælde.

Beredskab

Hvis et angreb bryder gennem alle de barrierer, der er stillet op, er det vigtigt at have forholdt sig til, hvordan man vil håndtere situationen. I mange tilfælde er der blot behov for at afklare mindre sikkerhedsmæssige spørgsmål og situationer via vores sikkerhedshotline, i andre tilfælde kan der være behov for et beredskab af eksperter, der kan træde til i en krisesituation hele døgnet.

Sikkerhedshotline
I denne pakke er vores eksperter til rådighed i form af en gratis sikkerhedshotline, hvor jeres teknikere og superbrugere kan få afklaret sikkerhedsmæssige spørgsmål i normal arbejdstid. Egentlige analyser vil afregnes på normale vilkår.

Beredskab til geninstallation
IT Relation vedligeholder et beredskab af teknikere, der kan bistå med retablering af software på udstyr, der er angrebet. Servicen dækker normal arbejdstid - med mindre der tegnes anden aftale.

Genskabelse

Geninstallation af angrebne klienter (laptops, PC'er o.lign.)
Hvis I efter et sikkerhedsangreb får behov for at retablere software på en eller flere angrebne klienter, vil vi bistå i dette arbejde uden yderligere beregning, i samme omfang som ved etablering af nyt udstyr.

Opfølgning

Efter et større angreb er det vigtigt at følge op på de sikkerhedstiltag, der er gjort og selve processen under og efter angrebet for at undgå gentagelser i fremtiden.

Ekstra review
Som en del af pakken tilbyder vi i disse tilfælde et ekstra review sammen med jer, hvor vi går forløbet igennem og kommer med forslag til forbedringer.

Regelmæssige aktiviteter

Review med aftalte intervaller
I de regelmæssige reviews checker vi om opsætningen af de ovennævnte elementer stadig er hensigtsmæssig, og vi kommer med forslag til overvejelser og forbedringer. Vi deltager ligeledes på et møde i jeres sikkerhedsudvalg.

OPTION: **Awarenes test**
Vi udsender regelmæssigt spørgeskemaer til jeres medarbejdere for at kontrollere deres paratviden indenfor awarenes. Indholdet kan evt. koordineres med jeres egne politikker.

OPTION: **Fishing test**
Vi udsender regelmæssigt mails til jeres medarbejdere, der ligner typiske fishing eller malware-mails for at evaluere i hvor høj grad de er opmærksomme på hensigtsmæssig adfærd.

Serversikkerhed

Beskyttelse

Antivirus/malware-beskyttelse
Antivirus/malwarebeskyttelse beskytter generelt mod uautoriserede programmer (orme, trojanske heste, adware, spyware mm.), der kan genere eller forsage skade. Beskyttelsen sker ud fra malware-databaser, der løbende opdateres online. Malwarebeskyttelses-programmet installeres i servermiljøet og på de enkelte servere.

Patch Management
Al software indeholder sårbarheder eller fejl i større eller mindre grad. Det er derfor vigtigt altid at være fuldt opdateret, så man får gavn af vigtige rettelser, der ellers kan udnyttes af IT-kriminelle. Patch Management er generelt en service, der allerede er inkluderet i hovedaftalen. I denne pakke kan den udvides med standard-serverapplikationer efter aftale med jer. Servicen inkluderer ikke deciderede opgraderinger af software.

Firewall
I ethvert servermiljø indgår i dag en firewall, der beskytter mod adgang for uvedkommende til andre services, end de der specifikt ønskes adgang til.
Vedligeholdelse af opsætningen af firewallen er en del af denne pakke, hvis den ikke allerede er etableret via hovedaftalen.

Advanced malware protection
En yderligere sikring mod uautoriserede programmer, der bl.a. følger og overvåger filer og programmer for uhensigtsmæs-sig opførsel. Grundlaget for disse vurderinger opdateres løbende i cloud baserede services, og belaster derfor serveren minimalt.

Multifaktor autentificering
Brugernavn og password alene er i mange tilfælde ikke længere tilstrækkelig sikring. Vi tilbyder derfor i denne pakke mulighed for to-faktor autentificering ved login på serverne. Den ekstra sikring sker bl.a. ved, at der kan sendes en sms med en engangskode.

Reset password
Vores Service Desk kan normalt resette jeres password, hvis I har glemt det. Med denne reset password service kan brugeren selv gøre det. Det giver en højere grad af sikkerhed i processen, og hurtigere adgang igen på alle tider af døgnet.

DNS-filtrering
Mange angreb starter med, at brugeren klikker på et link i en e-mail eller på en hjemmeside. DNS-filtrering sikrer, at man ikke kan komme ind på de sider, der allerede er kendt for at indeholde malware. Databaserne opdateres kort efter opdagelse af nye trusler. Servicen kan overvåges og styres centralt.
DNS-filtrering etableres på serveren og trækker på en fælles service med den opdaterede database over malware hjemmesider.

Overvågning

De beskyttelsesprodukter vi anvender indeholder i dag næsten alle et kontrolværktøj. Ved at vi overvåger alle produkterne samlet, kan vi opdage angreb og uhensigtsmæssigheder så tidligt som muligt.

Dette er en væsentlig fordel i at samle produkterne i en pakke, idet en overvågning af produkterne enkeltvis ikke giver de fulde billede.

Overvågning
Overvågningen, der er delvist automatisk og delvist manuel, kan f.eks. afdække, at bestemte servere er særligt udsatte. Hvis vi opdager alvorlige problemer, vil vi følge op og løse dem i fællesskab med jer. Der kan yderligere installeres et "cloud malware protection" program på serverne, der sikrer, at data om installeret software mm. indgår i overvågningen, og det kan bl.a. vise, hvilket udstyr, der er angrebet, hvis det først senere viser sig at være ondsindet software. Oplysningerne kan også anvendes i de regelmæssige reviews. Overvågningen dækker alle de beskyttelsesprodukter, der er indeholdt i pakken.

Eskalering
Hvis der ifm. overvågningen eller den regelmæssige scanning opdages kritiske sårbarheder behandles og eskaleres de på linje med driftsafbrydelser o.lign. Dvs. vi tager kontakt til jer og sammen vurderer truslen og evt. aktiviteter til imødegåelse.

OPTION: **Intrusion detection/ prevention i servernetværk**
Udstyr placeret i netværket, der overvåger netværkstrafikken, kan detektere tegn på indbrud i netværket, som er kommet gennem den øvrige beskyttelse og ikke er opdaget af den øvrige overvågning. Udstyret kan dels give alarm og dels stoppe eller begrænse angrebet i mange tilfælde.

Beredskab

Hvis et angreb bryder gennem alle de barrierer, der er stillet op, er det vigtigt at have forholdt sig til, hvordan man vil håndtere situationen. I mange tilfælde er der blot behov for at afklare mindre sikkerhedsmæssige spørgsmål og situationer via vores sikkerhedshotline, i andre tilfælde kan der være behov for et beredskab af eksperter, der kan træde til i en krisesituation hele døgnet.

Sikkerhedshotline
I denne pakke er vores eksperter til rådighed i form af en gratis sikkerhedshotline, hvor jeres teknikere og superbrugere kan få afklaret sikkerhedsmæssige spørgsmål i normal arbejdstid. Egentlige analyser vil afregnes på normale vilkår.

Beredskab til geninstallation
IT Relation vedligeholder et beredskab af teknikere, der kan bistå med retablering af servere, der er angrebet. Servicen dækker normal arbejdstid – med mindre der er tegnet anden aftale.

Genskabelse

Geninstallation af angrebne servere
Hvis I efter et sikkerhedsangreb får behov for at retablere servere og data, vil vi bistå i dette arbejde uden yderligere beregning.

Opfølgning

Efter et større angreb, er det vigtigt at følge op på de sikkerhedstiltag, der er gjort og selve processen under og efter angrebet for at undgå gentagelser i fremtiden.

Ekstra review
Som en del af pakken tilbyder vi i disse tilfælde et ekstra review sammen med jer, hvor vi går forløbet igennem og kommer med forslag til forbedringer.

Regelmæssige aktiviteter

Regelmæssig sårbarhedsscanning
Med jævne mellemrum scannes alle de aftalte servere og domæner for sårbarheder. I får tilsendt en rapport, som giver overblik over situationen.

Review med aftalte intervaller
I de regelmæssige reviews, checker vi om opsætningen af de ovennævnte elementer stadig er hensigtsmæssige, gennemgår seneste sårbarhedsscanning, og kommer med forslag til overvejelser og forbedringer, samt deltager på et møde i jeres sikkerhedsudvalg.

Audit
I forbindelse med de regelmæssige reviews, tilbyder vi sammen med jer at checke op på konfigureringen af jeres audit logs og at tage stikprøver af brugeropsætning, logins og adgang til jeres systemer. Dette kan afsløre systematisk tilsidesættelse af IT-sikkerhedspolitikker, procedurer o. lign.

Test af genetablering
Op til et regelmæssigt review tilbyder vi sammen med jer at teste restore af jeres systemer og data. Vi etablerer nye virtuelle servere i et beskyttet miljø, hvorefter jeres backup lægges ind, og I kan verificere, at alt er som det skal være.

Fortrolighed

Beskyttelse

Løbende awareness uddannelse af medarbejdere
For at beskytte fortrolige oplysninger, er det ekstra vigtigt, at alle relevante medarbejdere er informeret om risiko og fornuftig adfærd.
Vi tilbyder derfor en regelmæssig analyse af medarbejdernes vidensniveau (online spørgeskema m. evaluering) og gå-hjem-møder.

Sikker mail løsning med Outlook plugin og tunnelkryptering
Mange virksomheder og myndigheder anvender i dag sikker mail til at kommunikere fortrolige oplysninger via almindelig mail. Det er en fleksibel og sikker kommunikationsform. Et Outlook plugin sikrer bl.a., at brugeren let kan se, om der kan sendes sikkert til modtageren. Tunnelkryptering sikrer, at alle mails krypteres automatisk, uanset om man bruger Outlook plugin eller ej. Det kræver blot, at modtageren har et kompatibelt sikker mail-ststem fra en af de leverandører, der støtter op om standarden. Der er pt. over 600 maildomæner på den officielle liste, og det omfatter med meget få undtagelser alle offentlige myndigheder. Løsningen kan evt. udvides til at kunne sende fortroligt til private personer i eBoks.

Data leak/loss prevention "light"
Der findes forskellige teknikker til at forhindre, at virksomhedens data bevidst eller hændeligt sendes eller kopieres. I dette tilfælde anvendes en udvidelse af jeres mailscanning, der kan sikre, at oplysninger med åbenlyse CPR-numre og/eller lign. simple elementer ikke sendes videre. Der kan udvides med mere avancerede tiltag.

Virtuelt Privat Netværk - VPN
Når der udefra kobles op til virksomhedens netværk og servere vil en VPN-løsning kryptere al trafik og dermed beskytte mod at uvedkommende kan aflure informationerne.
VPN etableres på de enkelte enheder og i netværksudstyret, og adgangen kan styres med brugerens almindelige login.

OPTION: **Digital signering**
Fortrolige oplysninger på papir er meget vanskelige at styre sikkerhedsmæssigt. Mange aftaler og kontrakter kan derfor med fordel underskrives digitalt. Kontrakterne kan herefter opbevares i et beskyttet arkiv med sikkerhed for også at kunne dokumentere underskrifternes ægthed efter flere år.

OPTION: **Password Management**
I dag skal medarbejdere huske skiftende passwords på mange systemer og kravene til passwords er i dag så store, at de næsten er umulige at huske. Med Password Management kan man på en sikker måde opbevare passwords, og alligevel let anvende dem – i mange tilfælde uden at de bliver synlige under brug.
I nødstilfælde er det muligt for betroede medarbejder at få adgang til kritiske passwords ifm. sygdom eller fratrædelser.

Overvågning

De beskyttelsesprodukter vi anvender indeholder i dag næsten alle et kontrolværktøj. Ved at vi overvåger alle produkterne samlet kan vi opdage angreb og uhensigtsmæssigheder så tidligt som muligt.
Dette er en væsentlig fordel i at samle produkterne i en pakke, idet en overvågning af produkterne enkeltvis ikke giver de fulde billede.

Overvågning af sikker mail løsningen
Overvågningen, der er delvist automatisk og delvist manuel, kan f.eks. afdække, at jeres sikker-mail system ikke er opdateret med de korrekte certifikater fra jeres samarbejdspartnere. Hvis vi opdager alvorlige problemer vil vi følge op og løse dem i fællesskab med jer. Oplysningerne fra overvågningen kan også anvendes i de regelmæssige reviews.
Overvågningen dækker alle de beskyttelsesprodukter, der er indeholdt i pakken.

Eskalering
Hvis der ifm. overvågningen opdages kritiske sårbarheder behandles og eskaleres de på linje med driftsafb rydelser o.lign. Dvs. vi tager kontakt til jer og sammen vurderer truslen og evt. aktiviteter til imødegåelse.

Beredskab

Hvis et angreb bryder gennem alle de barrierer, der er stillet op, er det vigtigt at have forholdt sig til, hvordan man vil håndtere situationen. I mange tilfælde er der blot behov for at afklare mindre sikkerhedsmæssige spørgsmål og situationer via vores sikkerhedshotline, i andre tilfælde kan der være behov for et beredskab af eksperter, der kan træde til i en krisesituation hele døgnet.

Sikkerhedshotline
I denne pakke er vores eksperter til rådighed i form af en gratis sikkerhedshotline, hvor jeres teknikere og superbrugere kan få afklaret sikkerhedsmæssige spørgsmål i normal arbejdstid. Egentlige analyser vil afregnes på normale vilkår.

Beredskab til analyse af mail-flow
IT Relation vedligeholder et beredskab af teknikere, der kan bistå med analyse af mail-flow, hvis bestemte sikre mails er forsinket eller ikke kommer igennem. Servicen dækker normal arbejdstid, med mindre der er tegnet anden aftale.

Genskabelse

Almindelig genskabelse af data er ikke en del af denne pakke, men er normalt indeholdt i hovedaftalen.

Manuel gensendelse af sikre mails
Hvis sikre mails pga. fejl hos eksterne parter el.lign. ligger i kø og ikke umiddelbart kan sendes eller modtages korrekt, kan vi tilbyde at gensende dem manuelt, hvis muligt efter fejlsituationen er udbedret. Dette arbejde udføres uden yderligere beregning.

Opfølgning

Efter et større angreb, er det vigtigt at følge op på de sikkerhedstiltag, der er gjort og selve processen under og efter angrebet for at undgå gentagelser i fremtiden.

Ekstra review
Som en del af pakken tilbyder vi i disse tilfælde, et ekstra review sammen med jer, hvor vi går forløbet igennem og kommer med forslag til forbedringer.

Regelmæssige aktiviteter

Review med aftalte intervaller
I de regelmæssige reviews checker vi om opsætningen af de ovennævnte elementer stadig er hensigtsmæssige og kommer med forslag til overvejelser og forbedringer, samt deltager på et møde i jeres sikkerhedsudvalg.

Audit
I forbindelse med de regelmæssige reviews, tilbyder vi sammen med jer at tage stikprøver af anvendelsen af sikre (eller ikke sikre) mails. Dette kan afsløre uhensigtsmæssig og systematisk tilsidesættelse af IT-sikkerhedspolitikker, procedurer o. lign.

OPTION: **Data Discovery**
Trods omhyggelig efterlevelse af retningslinjerne, er der en risiko for, at fortrolige oplysninger placeres uhensigtsmæssigt. Med Data Discovery er det muligt at scanne bl.a. PC'er og netværksdrev for kritiske kategorier af data, f.eks. personoplysninger eller fortrolige forretningsdata.

IT-sikkerhed med fokus på forretningen

Vi arbejder med IT-sikkerhed ud fra et forretningsmæssigt perspektiv. Vores erfaring er, at du med effektive IT-sikkerheds-løsninger ikke alene slipper for frygten for IT-kriminalitet – du får også frigjort forretningsmæssige potentialer.

Garanti for sikker IT
Vi er certificerede til at bruge Hostingmærket. Det er din garanti for, at vi lever op til strenge IT-sikkerhedskrav.

Fantastisk support
Få altid adgang til IT-support. 24 timer i døgnet. Hver dag. Året rundt. Vi er der for dig, hvis du får brug for os.

Forretning før løsning
Vi snakker altid forretning, før vi snakker IT-sikkerhedsløsning. Det sikrer dig en optimal beskyttelse af din forretning.

Er din virksomhed optimalt beskyttet mod IT-kriminelle?

Lad os tage en uforpligtende snak om, hvordan vi kan forbedre IT-sikkerheden i din virksomhed.

Ønsker du at høre mere?
Kontakt din Client Manager, eller Business Relation Manager:

Martin Reinholdt
marei@itrelation.dk
+45 2447 9737

Herning
Dalgas Plads 7B, 1. sal
7400 Herning

Aarhus
Søndervangs Allé 20
8260 Viby J

Hellerup
Kildegårdsvej 20
2900 Hellerup

København
Artillerivej 90, 1 sal
2300 København S