GUIDE

VÄGEN TILL EN MOBIL OCH SÄKER ARBETSPLATS

Din guide till modern IT-säkerhet för det moderna företaget

ADDPRO

DET MOBILA FÖRETAGET

– nya möjligheter och nya utmaningar

Drivkraften bakom många företags digitalisering och molnsatsningar är möjligheten att kunna erbjuda sina medarbetare ett mer mobilt och flexibelt arbetssätt.

Idag uppskattar de flesta av oss att kunna jobba utan att vara bundna till det fysiska kontoret eller till fasta kontorstider. Inte minst yngre generationers medarbetare förväntar sig att kunna jobba när de vill, där de vill. Självklart utan att ge avkall på det IT-stöd och de digitala verktyg som är en förutsättning för ett flexibelt och modernt arbetssätt.

När kontoret går från att vara en arbetsplats till att bli en mötesplats och arbetslivet smälter samman med privatlivet ställs nya krav på företagets säkerhet. Den traditionella synen på IT-säkerhet räcker helt enkelt inte till när arbetsplatsen är spridd över en mängd enheter och geografiska platser och informationen i allt högre grad finns i molnet. För att kunna skydda sina medarbetare, deras arbetsverktyg och sin information på ett fullgott sätt behöver det moderna företaget en lösning för modern IT-säkerhet.

I guiden tittar vi närmare på hur det moderna arbetssättet ställer nya krav på företagets IT-säkerhet. Vi reflekterar också över hur du som IT-ansvarig eller företagsledare kan tänka och gå till väga för att säkra upp företaget i en alltmer mobil och flexibel värld.

SEX TRENDER SOM ÖKAR KRAVET PÅ MODERN IT-SÄKERHET

Det moderna arbetssättet påverkar kraven på IT-säkerhet på flera sätt. Här tittar vi närmare på sex aktuella drivkrafter som ställer krav på ett nytt sätt att arbeta med IT-säkerhet.

Fler mobila användare med allt fler mobila enheter

I takt med att allt fler väljer att arbeta mobilt och utanför kontorets väggar ökar användningen av mobila verktyg. Vi väljer den enhet som passar bäst för stunden. Inne på kontoret är det förmodligen en dator som företaget tillhandahåller och som IT-avdelningen har kontroll över. På bussen eller på ett café kan det vara mer tilltalande att använda surfplattan eller mobilen. Hemma kan det var lockande att arbeta på barnens speldator, den mest kraftfulla i hela huset. Ofta har vi som slutanvändare inte klart för oss vilka enheter som kan anses vara säkra. Något så enkelt som en borttappad telefon eller surfplatta, med dåligt skydd för information och applikationer, kan utgöra en stor säkerhetsrisk.

Mer kommunikation sker i molnet

Vi bär inte bara med oss våra arbetsverktyg vart vi går, vi förväntar oss också att kunna koppla upp oss och arbeta oavsett var vi befinner oss. Det kan vara så harmlöst som att kunna kolla mejlen på bussen eller läsa servicerapporter hemma i soffan. Men hur skyddat är egentligen ett hemmanätverk mot angrepp och intrång och vilka har tillgång till nätverket? Mot vilka nät kopplar vi upp våra mobila enheter, vilka appar används och krypterar de data på ett tillfredställande sätt? När vi kan komma åt våra jobbmappar var vi än befinner oss har alla andra i hela världen en teoretisk möjlighet att också komma åt samma information. All kommunikation över osäkra nätverk ökar risken för angrepp.

Vi delar information som aldrig förr

Vi delar filer som aldrig förr. Det finns alltid en risk att filer som mejlas fram och tillbaka till sist hamnar i fel inkorg. Dokument tankas upp i molnet till en publik lagringstjänst och delas vidare med en öppen länk. Länken mejlas vidare utan en tanke på att alla som kommer över länken har full access. När vi oförsiktigt delar filer i molnet finns risken att de sprids långväga och aldrig kan hämtas tillbaka.

När vi oförsiktigt delar filer i molnet finns risken att de sprids långväga och aldrig kan hämtas tillbaka.

Kvalificerade lösenord invaggar oss i falsk trygghet

Att de flesta online-tjänster och molnservrar kräver kvalificerade lösenord är ingen garanti för god IT-säkerhet. Ofta skrivs inloggningsuppgifter ner på papperslappar och i okrypterade dokument som lagras lite varstans. Det finns mängder med plugins och appar som sparar användarnamn och lösenord under ett master-konto bortom IT-avdelningens kontroll. Det absolut vanligaste snedsteget när det kommer till lösenord och säkerhet är ändå att vi använder samma inlogg och lösenord till flera applikationer och tjänster. Blir en server eller tjänst hackad, är risken stor att alla andra också är hackade i samma sekund.

Användningen av skugg-IT fortsätter att öka

När IT-avdelningen inte lyckas erbjuda moderna lösningar som lever upp till medarbetarnas förväntningar är risken stor att medarbetare tar saken i egna händer. Att dela filer på Dropbox eller iCloud, samarbeta i Slack eller chatta över Messenger är ett billigt och enkelt sätt att förbättra samarbete med kollegor och kunder. Problemet är att alla dessa molntjänster är bortom IT-avdelningens kontroll. När allt fler väljer att lagra eller dela företagsdata och affärskritisk information i dessa skugg-IT-applikationer ökar säkerhetsrisken. Så snart en fil sparas i en molntjänst utanför företaget uppstår också frågan vem som ansvarar för innehållet, att säkerhetsbackuper görs. Vad händer om någon slutar? Vem raderar filer och säkerställer att senaste versionen finns på företagets server?

Den mörka sidan av IT växer snabbt

Parallellt med nya modernare arbetssätt och mer mobila medarbetare växer den mörka sidan av IT snabbt – så snabbt att den idag omsätter mer än narkotikahandeln. Hur många ID- och användarkapningar som sker vet ingen. Det enda som är säkert är att mörkertalet är stort och att antalet angrepp ökar. Och det är inte bara stora kända företag som utsätts för attacker, även mindre företaget är i farozonen. Botar ligger och letar efter inloggningsuppgifter som läckt ut och på den mörka sidan av internet säljs listor från hackade servrar. Med den dåliga vanan att använda samma inloggning på flera ställen öppnar en sådan lista upp många dörrar som borde vara stängda. I molnet behövs en högre nivå av säkerhet med skydd mot ransomware och ID-kapning med möjligheten att snabbt upptäcka avvikande beteenden.

ATT SÄKRA UPP DEN MOBILA ARBETSPLATSEN

Det moderna företaget, med mobila medarbetare, behöver modern IT-säkerhet. Det är inte en engångsinsats med en ny brandvägg och uppdaterad lösenordspolicy. Istället är det ett löpande arbete med utgångspunkt i hur medarbetarna jobbar och vilka verktyg de använder. I grunden handlar modern IT-säkerhet om att säkra användarnas konton, hantera enheter och att skydda data i molnet.

Säkra individens identitet och användarkonto

Det första och viktigaste steget är att skydda användarnas identitet, det vill säga deras konton och inloggningsuppgifter. Läcker användaruppgifter ut finns det risk för att affärskritisk information om kundrelationer, ledningsbeslut och budgetar hamnar i fel händer.

Nyckeln är att ha en lösning som säkerställer att varje användare verkligen är den de utger sig för att vara och att alla kan vara trygga i att de vet vem de kommunicerar med. En tydlig lösenordspolicy och att säkra varje inloggning med tvåfaktorautentisering är bra första steg. Det handlar också om att ha koll på vilka rättigheter varje individ har, vilka enheter, appar och tjänster användaren ska ha behörighet till.

Säkra alla mobila enheter

Med allt fler mobila arbetsverktyg blir det också viktigt att kunna kontrollera och skydda även dessa. Det gäller för IT-avdelningen att ha koll på vilka enheter som används och av vem, så att inte fel personer kommer åt företagets system och data. Det handlar också om att kunna styra vilka applikationer och vilken information som ska få användas på vilka enheter. Att sätta upp riktlinjer för vilka enheter som får access till företagets servrar och tjänster bidrar till att öka säkerheten och minska risken att informationen får fötter. På samma sätt gäller det att snabbt kunna låsa eller radera känsligt innehåll på en enhet som kommit på villovägar.

Säkra filer och data

När data blivit det nya guldet och en affärskritisk resurs för företaget är det också viktigt att säkra upp den digitala informationen. Att säkra företagsdatan handlar dels om att säkerställa att bara den som ska komma åt en viss typ av information kan göra det – i praktiken att klassificera datan och tilldela behörigheter. Det handlar också om att styra på vilket sätt filer ska kunna skickas vidare eller sparas, lokalt och i molnet.

Att ha bra rutiner för hur och hur ofta informationen ska backas upp för att inte gå förlorad är en annan viktig del av arbetet. Och hur snabbt den ska kunna återställas om någon av misstag raderar en fil eller ett kryptovirus attackerar och förstör viktig information.

…men inte på bekostnad av användarvänligheten

Traditionellt har IT-säkerhet och användarvänlighet setts som varandras motsatser. Ökad säkerhet har lett till nya begränsningar i de anställdas vardag. Risken är stor att komplicerade säkerhetsrutiner resulterar i att användningen av skugg-IT växer.

Modern IT-säkerhet handlar om att skydda företagets medarbetare, enheter och data, utan att försämra användarupplevelsen. Idag finns också alla möjligheter att säkra upp företaget på ett användarvänligt sätt så att säkerheten blir en trygghet – inte ett hinder.

SÅ VISAR MICROSOFT VÄGEN TILL MODERN IT-SÄKERHET

För den som väljer Microsoft för sin IT-miljö finns idag riktigt goda möjligheter att säkra upp verksamheten. För att kunna erbjuda den säkerhetslösning som är rätt för just ditt företaget och dina användare erbjuder Microsoft säkerhetsfunktioner på olika funktionalitets- och licensnivåer. Förenklat kan det beskrivas som en trappa.

Steg 1 – Windows 11 lägger grunden för modern IT-säkerhet

Många företag använder tyvärr fortfarande äldre operativsystem och installerar inte säkerhetsuppdateringar i takt med att de släpps. En uppgradering till Windows 11 är det första steget mot ett bättre IT-skydd. Genom att aktivera Windows 11 inbyggda virusskydd och brandvägg får företaget ett grundläggande skydd. Ett litet steg som gör skillnad.

Steg 2 – Bättre produktivitet och säkerhet med Office 365

Många förknippar Office 365 med alla de applikationer som gör arbetet och samarbetet smidigare och mer eff ektivt, från Word, Excel och Powerpoint till Teams, Yammer och SharePoint. Office 365 innehåller också en rad säkerhetsfunktioner såsom tvåfaktorautentisering, möjligheten att kryptera fi ler som sparas i OneDrive och stöd för att implementera en lösenordspolicy på företaget. I mejlservern Exchange kan du sätta upp regler för mejlhantering och aktivera skydd mot intrång, trojaner och annan skadlig kod.

Så länge du rör dig innanför företagets brandväggar och arbetar mot företagets lokala servrar arbetar du tryggt och säkert i Windows 11 och Office 365. När allt mer arbete flyttar ut i molnet och arbetsplatsen har blivit mobil räcker inte säkerheten i Office 365 hela vägen.

Steg 3 – Microsoft 365 tar säkerheten hela vägen

Bästa sättet att skydda användare, deras mobila enheter och data fullt ut är att uppgradera till Microsoft 365. I Microsoft 365 ingår Office 365, Enterprise Mobility + Security (EMS) och Windows 11 med tillhörande säkerhetsverktyg. Med hjälp av identitetshanteringen i Azure Active Directory (AD) får IT-avdelningen kontroll över användarens rättigheter och vilka enheter och appar som används. Azure AD erbjuder också skydd mot att okända personer loggar in på användarens konto från en mobil enhet genom att larma och kräva tvåfaktorautentisering.

Verktyget Microsoft Intune som ingår i EMS hjälper till att hantera och säkra de enheter som används i företaget. Med Intune hanterar du allt från mobiler och surfplattor till bärbara datorer men också vilka appar som får användas. Intune gör det också möjligt att låsa eller radera känsligt innehåll på enheter som kommit på villovägar.

Azure Information Protection används för att klassifi cera känslig data, manuellt eller per automatik med hjälp av regler som till exempel. kan leda till behörighetskontroll, kryptering och spårning. I Microsoft 365 Cloud App Security kan du styra om fi ler ska kunna sparas ner lokalt eller till en viss molntjänst eller inte, med automatisk dataskyddskontroll som varnar ifall stora mängder data raderas eller laddas ned.

Kräver ditt företag ytterligare säkerhet är Windows Defender Advanced Threat Protection (ATP) ett tillägg till Microsoft 365. ATP drar nytta av Artifi ciell Intelligens och Machine Learning för att på ett intelligent sätt avvärja hot. ATP lär sig dina användares rutiner och reagerar om något bryter mot mönstret. Tjänsten lär sig också att upptäcka externa hot och hantera dem per automatik.

AddPro hjälper dig säkra upp företaget

Vi på AddPro brinner för att hjälpa företag säkra upp sin verksamhet med modern IT-säkerhet. Vi är ett kunskapsföretag som utvecklar säkra, flexibla och kostnadseffektiva IT-system. Våra 300 konsulter runt om i Sverige hjälper dagligen företag skydda sina användare, sina enheter och sin data. Vi har gedigen kunskap om möjligheterna med Microsoft 365 och hur du bäst drar nytta av tvåfaktorautentisering, kryptering och enhetshantering i ditt säkerhetsarbete. Tillsammans hjälper vi dig hitta möjligheterna för hur ditt företag kan jobba mobilt och flexibelt utan att ge avkall på företagets IT-säkerhet.

Hör av dig om du vill veta mer!

AddPro
solutions@addpro.se
040 59 24 00
www.addpro.se

ADDPRO