

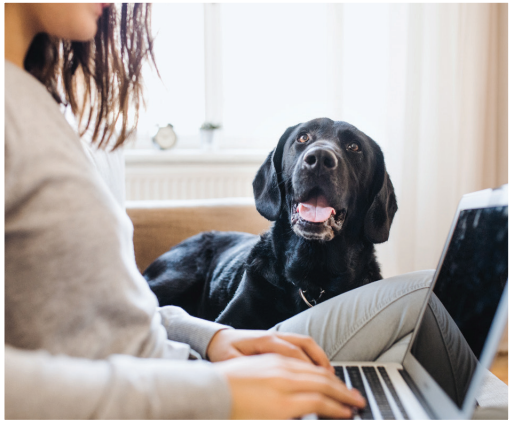

Lärdomar från covid-19: Planering för säkerhet och kontinuitet

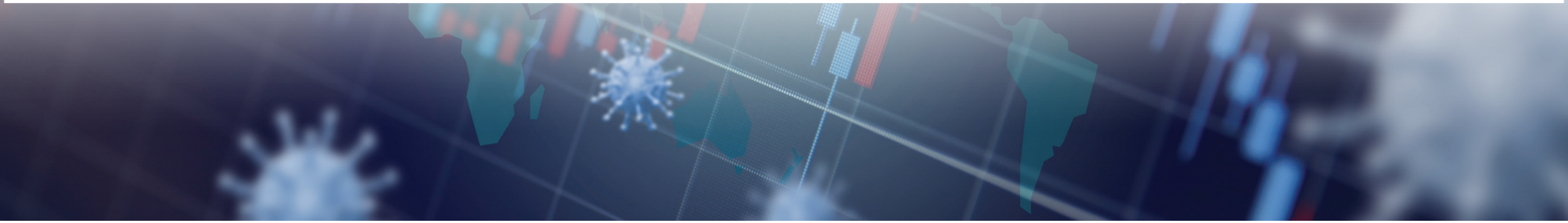
Innehållsförteckning

INLEDNING

Samhället har ställts inför en stor pandemi. Det nya coronaviruset (covid-19) påverkar nästan alla människor i hela världen. Skolor stängs, resandet begränsas, evenemang ställs in och kontor töms – allt detta i syfte att bromsa spridningen av covid-19. Centret för sjukdomsbekämpning har till och med föreslagit att arbetsgivare ska införa policyer som gör det möjligt för de anställda att arbeta på distans som ett sätt att främja social distansering. Företagen har följt uppmaningen och snabbt mobiliserat sig för att möta hotet, vilket har lett till att fler människor än någonsin tidigare i modern historia arbetar hemifrån. Låt oss ge en känsla för hur stor omvälvning det kan vara. Enligt en studie har mängden distansarbetare i Amerika ökat med 159 % mellan 2005 och 2017. I dag kan vi med säkerhet säga att vi nu, på grund av coronavirusutbrottet, har att göra med betydligt många fler.

Åtgärderna på grund av coronaviruset är något helt nytt, och för många företag innebär ”experimentet” att arbeta hemifrån att man tvingas ut på okänd mark. I denna e-bok beskriver vi strategierna för att upprätthålla affärskontinuiteten under coronavirusutbrottet.





LÄGESANALYS I LJUSET AV COVID-19:
NUVARANDE UTMANINGAR FÖR AFFÄRSKONTINUITET

Varje dag ställs vi inför säkerhetsrisker inom IT. En av utmaningarna med att möjliggöra rörlig arbetskraft är att detta dock kraftigt kan öka risken att utsättas för IT-attacker. Utan fördelen med skyddet hos ert kärnnätverk kan användare på språng smittas av datorvirus utan er vetskap och till och med föra in smittan bredare i er miljö när de senare åter kopplar in sig i nätverket.

Hackare drar nytta av rädslan för coronaviruset

Det verkar som om hackare drar nytta av alla större nyheter eller evenemang på världsnivå för att lansera sina attacker. I stunder av förhöjd rädsla kommer era anställdas e-post och konton i sociala media att fyllas med nyheter, kommentarer, videoklipp och länkar om viruset. Tyvärr utnyttjar IT-brottslingar rädslan till att utsätta era användare för phishing, hacka sig in i deras system eller installera skadeprogram.

Här är bara några få exempel på hur angripare drar nytta av coronaviruset:

- **Utger sig för att representera Världshälsoorganisationen** (WHO). WHO har rapporterat om misstänkta phishing-meddelanden som utgav sig för att komma från dem och påstod sig innehålla mycket viktig hälsoinformation. Måltavlorna ombads att klicka på en länk och ladda ner en fil eller uppge känslig information.

- **Leverans av skadeprogram**. En hackargrupp har utnyttjat coronapandemin till att infektera offer i Mongoliet med tidigare okänd skadlig kod, i en nyligen upptäckt kampanj kallas den ”Vicious Panda”.

- **Spam med trojanen Emotet**. Hackare använder till synes nyttiga meddelanden till japanska användare om hur man förhindrar spridningen av coronavirus som en del av en spam-kampanj med målet att installera trojanen Emotet. Emotet kan ta över e-postkonton och skicka falska meddelanden för att ännu djupare infiltrera en miljö.

- **Falsk app för smittspårning installerar utpressarprogram.** En app som hävdade att den lät dig på kartan följa utbrott av coronaviruset var egentligen ett utpressarprogram som blockerade din telefon. Appen ”COVID19 Tracker” infekterar din enhet och kräver 100 USD i Bitcoin inom 48 timmar.

Nybörjare på att arbeta utanför nätverket

COVID-19 har lett till uppkomsten av aggressiva policyer för arbete hemifrån, där företag nästan över natten stänger sina kontor och skickar hem de flesta av sina anställda för att arbeta hemifrån. Även om flexibelt arbetssätt nu är normen hos många företag brukar hos ett genomsnittligt företag vid varje given tidpunkt endast cirka 30 procent av medarbetarna arbeta hemifrån. Många företag har fått kämpa för att kunna tillhandahålla de resurser som behövs för att hålla medarbetarna säkra medan de arbetar hemifrån, genom att snabbt distribuera bärbara datorer eller genom att skicka hem anställda med stationära datorer som aldrig var tänkta att användas utanför företagets säkrade nätverk. Datorerna behöver inte bara säkerhet nu, i och med att de befinner sig utanför nätverket. Det är också viktigt att se till att de inte introducerar skadeprogram eller andra hot när de ansluter till nätverket, antingen via VPN eller när de kommer tillbaka till kontoret.

VPN-kanalerna är överbelastade

När coronaviruset sprider ut de anställda för att arbeta hemifrån har VPN-användningen skjutit i höjden. Forskare har noterat en ökning med 50 % av trafiken över en vecka. Bara i USA förväntar man sig en ökning av VPN-användningen med 150 % på en månad. Den plötsliga migreringen av användare från företagets lokaler till hemmakontoret har gjort att många företag har ansträngt sig för att tillhandahålla VPN-licenser åt sina anställda. Risken är att utan VPN-anslutning kommer användarna inte att ha tillgång till resurserna de behöver, eller så kanske de kommer att använda osäkra anslutningar för att ansluta sig till dem.

Bandbreddskaos

Det är inte bara era anställda som arbetar hemifrån. När skolorna är stängda kommer många av era medarbetare att ha sina barn hemma, som fortsätter sin undervisning på distans, spelar spel eller helt enkelt surfar på webben. Både föräldrarna och barnen kommer snabbt att sluka bandbredden, i synnerhet om de använder resursintensiva tillämpningar, såsom videokonferenser. De platser som drabbats hårdast av viruset har upplevt ökad internetanvändning med över 90 %. Som svar på detta uppgraderar många internetleverantörer sina kunder till snabbare tjänster med större bandbredd, eller eliminerar begränsningarna i mängden data för att undvika överanvändning.

Användningen av VPN-kanaler

har skjutit i höjden:

en ökning på 50 % per vecka.

Bara i USA förväntar man sig en

ökning av VPN-användningen

med 150 % på en månad.

ÅTTA TIPS TILL IT-CHEFER OM HUR MAN ANVÄNDER SÄKERHET SOM ETT SÄTT ATT MÖJLIGGÖRA PRODUKTIVITET OCH ÅTKOMST

1. INVENTERA OCH BEDÖM FÖRETAGETS MÖJLIGHETER TILL DISTANSARBETE

Även om 92 % av företagen erbjuder distansarbete, har denna möjlighet inte erbjudits i samma omfattning till alla anställda. För många företag har omställningen till distansarbete skett nästan över en natt, vilket gav begränsad tid för tillräcklig planering. Nu behöver man granska och bedöma vilken ny nätverksåtkomst företaget behöver och överväga konsekvenserna för säkerheten. Leverantörer av hanterade säkerhetstjänster (MSSP/Managed Security Services Provider) är experter på säkerhetsbedömningar och kan hjälpa medelstora företag att snabbt komma igång och att ge användarna det de behöver.

För nätverksnomader som alltid är på språng är chansen stor att de redan har de resurser de behöver på längre sikt. För dem som inte har arbetat lika mycket hemifrån kan det vara nyttigt att inventera alla data och tillämpningar de behöver komma åt regelbundet. Sedan kan ni fortsätta med att kartlägga vad som behöver nås, vem som behöver vilken åtkomst och hur åtkomsten bäst ordnas. Samarbeta med avdelningscheferna för att förstå de unika behoven hos varje team och se till att deras teammedlemmar får rätt förutsättningar för att kunna lyckas.

Här är en checklista över saker man behöver tänka på:

- ✔ Har den anställde en godkänd enhet, eller behöver ni skaffa fler telefoner/bärbara datorer?
- ✔ Har du tillräckligt med VPN-licenser för att utfärda åtkomst till alla som behöver detta, eller behöver ni skaffa fler?
- ✔ Har medarbetaren tillräckligt god internet-anslutning för att kunna utföra sitt jobb?
- ✔ Vilka system behöver medarbetaren komma åt för att utföra sitt jobb?
- ✔ Kräver medarbetaren säkrad åtkomst till känsliga system och uppgifter?
- ✔ Vilka molnprogram brukar medarbetaren regelbundet använda?
- ✔ Är medarbetaren korrekt konfigurerad och utrustad för att kunna använda multifaktorautentisering?

2. ANGE OCH KOMMUNICERA FÖRVÄNTNINGARNA KRING DISTANSARBETET

Eftersom många av era anställda antagligen för första gången arbetar hemifrån är det ett bra tillfälle att informera ert team om företagets policy för hemarbete och fastställa företagets förväntningar på de anställda som arbetar på distans. Cirka 24 % av företagen har inte uppdaterat sina policyer för hemarbete på över ett år och detta är en god möjlighet att göra det. Ett enkelt e-postmeddelande eller ett konferenssamtal med hela teamet kan räcka långt.

Några saker som ni kanske vill ta upp:

- **Tillgänglighet** – Under vilken tid på dagen förväntar ni er att teamet ska arbeta? När kommer du själv att kunna nås?
- **Reaktionshastighet** – Förväntas det att en distansarbetare ska svara omedelbart? I så fall, hur kommer dessa förväntningar att kommuniceras? Som ett exempel: kommer riktigt brådskande förfrågningar endast att ske via telefonsamtal?
- **Plattformar** – Påminn era anställda om vilka verktyg och plattformar de ska använda, inklusive plattformar för molnlagring, kommunikation, videokonferenser, projektledning m.m. Uppmuntra ditt team att inte använda andra plattformar än de som är godkända.
- **Enheter** – Om ert team har erhållit enheter från företaget behöver ni påminna om eventuell användningspolicy som gäller för dessa. Om de anställda använder sina egna privata enheter för sitt arbete är nu ett bra tillfälle att ge vägledning om vilka enheter som är lämpliga att använda och hur de anställda bör sköta arbetet via dessa enheter.
- **Incidentrapportering** – Vart ska en anställd vända sig om de upplever att företagets information kan ha äventyrats? Till vem ska överträdelser rapporteras? Vilka åtgärder ska de vidta för att minimera negativa följder?

3. FRÄMJA EN KULTUR AV IT-SÄKERHET

De flesta företagsledare vet att kulturen på en arbetsplats i hög grad påverkar om företaget kommer att lyckas eller ej. De måste också förstå att samma koppling finns vad gäller IT-säkerheten. Eftersom era anställda riskerar att utsättas för riktade attacker, där kanske någon låtsas vara en medarbetare i ert team, blir det ofta så att företagskulturen utgör den avgörande skillnaden mellan att lyckas avstyra attacken eller att hela nätverket smittas.

Hackare använder tekniker för att manipulera och påverka era användare att göra det de önskar, med auktoritet och tidsbrist som argument. Som ledare bör du uppmuntra till öppen kommunikation, så att om en anställd, även längst ned i organisationen, ser något de tror kan vara ett hot upplever de att de har rätt att rapportera och att deras oro kommer att tas på allvar.

Tips för att främja en kultur av IT-säkerhet:

- **Dela berättelser.** Har någon anställd avslöjat ett phishing-meddelande eller fått sin bärbara dator infekterad med utpressarprogram? Om man berättar om detta inom företaget kan det bidra till att era anställda upplever hoten som verkliga och lyckas stå emot liknande angrepp. Det kan också vara till hjälp att rapportera om attacker mot liknande företag.
- **Belöna goda beteenden.** När en anställd rapporterar om en potentiell attack kanske de skyddar ert företag mot ett enormt problem. Varför inte ta och belöna deras insats? Om man uppmuntrar de anställda att rapportera misstänkt aktivitet kan detta bidra till ökad medvetenhet och engagera flera.
- **Var trevlig.** Låt oss inse att företag består av människor med mycket varierande teknikmogenhet. Det är helt enkelt inte realistiskt att tro att alla anställda kommer att undvika alla hot och följa varje policy. Människor gör misstag. Just av den anledningen är det så viktigt att stödja dem.

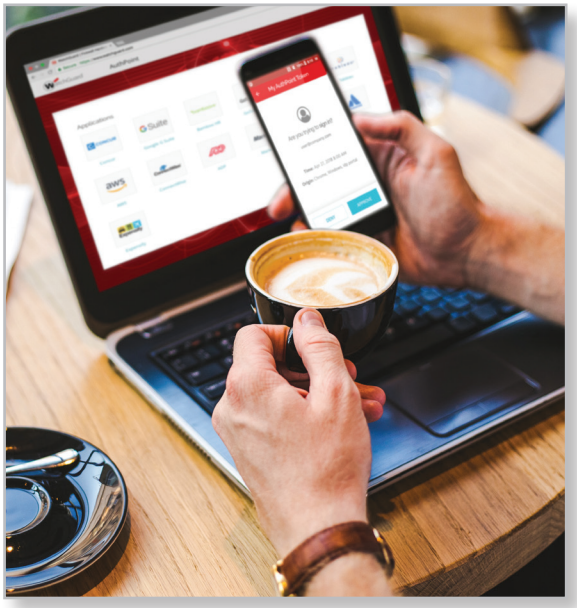
4. GENOMFÖR MULTIFAKTORAUTENTISERING

När företag brottas med att större delen av deras arbetskraft arbetar på distans blir det en stor utmaning att säkra tillgången till de interna verktygen. Samtidigt riktar hackare alltmer in sig på att komma över inloggningsuppgifter och siktar specifikt in sig på just detta. Därför rekommenderar vi att ni ordnar MFA (multifaktorautentisering) till alla era användare, så att alla autentiseras ordentligt varje gång de ansluter till nätverket.

Med multifaktorautentisering kan ni även skydda åtkomsten till molnprogram och miljöer som fjärrarbetare kan nå direkt från internet. Detta skapar ett extra lager av skydd vid ett tillfälle då företagen är extra sårbara.

Det här bör du efterfråga i er lösning för MFA:

- **Molnbaserat.** Till skillnad från MFA som bygger på hårdvarunycklar kan användaren med en molnbaserad lösning komma igång direkt genom att hämta och konfigurera ett program till sin telefon.
- **Programmets omfattning.** Lösningen ni väljer bör integreras så att den skyddar alla kritiska program som era anställda kan behöva.
- **Enkelhet.** Användningen av lösningen behöver vara intuitivt förståelig för användare med skiftande teknisk förmåga.
- **Flera olika autentiseringsmetoder.** Stöd för flera olika autentiseringsalternativ, både online och offline, säkerställer att de behöriga användarna kan komma åt allt de behöver när det behövs.
- **Stöd för flera olika nycklar.** MFA erbjuds nu ofta av sociala medier, banker, säljkanaler med flera. Försök att hitta en lösning som låter er konsolidera nycklarna i ett enkelt MFA-program för att ge användarna effektiv åtkomst.



5. UTÖKA VPN-ÅTKOMSTEN FÖR PRIORITERADE ANVÄNDARE

Säker anslutning till företagets kontor och kritiska program är avgörande för att era anställda ska kunna fortsätta vara produktiva när de arbetar på distans. VPN-tjänster (virtuella privata nätverk) skapar ett extra lager säkerhet för privata och publika nätverk och låter de anställda och andra organisationer skicka och ta emot data över internet på ett säkert sätt.

I allmänhet kommer era användare att behöva någon av två olika VPN-typer:

1. **Klientbaserad VPN.** En klientbaserad VPN-lösning verkar på nätverksnivån och ger användaren åtkomst till hela nätverket.

2. **Klientlös VPN.** En klientlös VPN-tjänst behöver vanligtvis bara en webbläsare och ger användaren åtkomst till utvalda program och tjänster.

Normalt tillhandahåller företag VPN endast till en begränsad grupp anställda som arbetar på distans och/eller ofta reser i tjänsten, till skillnad från hela personalen. När användningen av VPN kraftigt växer följer här några råd om hur ni kan hantera användningen och slippa störningar:

- **Prioritera först VPN till högriskanvändare**. Vissa anställda kommer att behöva bredare åtkomst än andra, medan andra kanske inte behöver någon VPN-anslutning över huvud taget. Att förstå vem som behöver åtkomst och till vad och att erbjuda VPN beroende på prioriteringar hjälper till att undvika överbelastning av nätverket.

- **Använd en molnbaserad brandvägg för att kunna hålla jämna steg med efterfrågan.** Den ökade efterfrågan på VPN-tjänster innebär inte att ni behöver frigöra mer plats i serverrummet. Molnbaserade brandväggar kan bidra med utjämning av belastningen i VPN-trafiken till huvudkontoret och kan storleksanpassas utifrån hur många anslutningar företaget behöver.

- **Ställ krav på MFA.** Om ni inte använder MFA kan en enda uppsättning inloggningsuppgifter till VPN-tjänsten ge en angripare full åtkomst till hela ert nätverk. Användare som ansluter via VPN bör vara komplett autentiserade med minst tvåfaktorautentisering.

- **Dela ut bordsbaserade brandväggar.** En bordsbaserad brandvägg som installeras i användarens hemmakontor kan ge komplett UTM-skydd utan att företagets VPN behöver belastas.

6. SKYDDA ANVÄNDARE MOT FARLIGA KLICK MED HJÄLP AV DNS-FILTRERING

Att skydda användarna när de surfar på nätet är svårare när de är uppkopplade utanför företagets nätverk. När de anställda sitter fast hemma är sannolikheten stor att företagets bärbara datorer kommer att användas till en hel del privat webbsurfning och läsning av e-post. Molnbaserad DNS-filtrering gör det möjligt att blockera anslutningar och begränsa åtkomsten till farliga platser på internet. Klick på skadliga länkar eller försök att koppla upp sig till domäner som används för phishing och skadlig kod kan förhindras, utan att man behöver använda VPN.

Saker att tänka på i en lösning för DNS-filtrering:

- **Produktivitet och genomdrivande av policyer.** När fler anställda arbetar utanför kontoret kanske ni även av produktivitetsskäl vill begränsa åtkomsten för era användare till vissa typer av innehåll på nätet, såsom sociala medier och webbplatser för vuxna. Leta efter möjligheter till detaljerad styrning, exempelvis möjligheter att blockera för vissa användare och grupper, och kanske att ange under vilka timmar på dagen policyn är tvingande.

- **Stöd till initiativ för säkerhetsutbildning.** Vid det här laget har de flesta företag någon form av utbildning i IT-säkerhet för sina anställda, men när de går över till distansarbete är det viktigare än någonsin att förstärka denna utbildning. Vissa lösningar för DNS-filtrering blockerar inte bara åtkomsten till skadliga platser utan påminner användaren om hur man känner igen liknande hot i framtiden.

7. HÅLL SLUTPUNKTERNA FRIA FRÅN SKADEPROGRAM

Coronaviruset har bara lett till att hoten från skadlig kod och ransomware har accelererat. Och risken att smittas har aldrig varit högre än nu, eftersom användare kanske inte längre skyddas av företagets brandvägg vid arbete hemifrån. Även om antiviruslösningar för slutpunkter kommer att fånga många hot, står de maktlösa mot skygga, tidigare aldrig sedda skadeprogram, något vi stöter på alltför ofta. EDR-lösningar (Endpoint Detection and Response) kan inte bara upptäcka dessa avancerade hot utan även stoppa hotet och återställa infekterade enheter till god ordning, allt helt på distans.

Viktiga funktioner i EDR-lösningar:

- **Detektionsmetoder.** För att fånga upp avancerad skadlig kod krävs avancerade tekniska lösningar. Leta efter lösningar som kombinerar flera detekteringsmetoder, inklusive analys av programbeteende, heuristisk analys och sandlådeanalys.

- **Automatisering och AI.** Man kan slippa många problem om man reagerar snabbt på hot. Automatisering av detektering och reaktion klarar att göra detta nästan omedelbart.

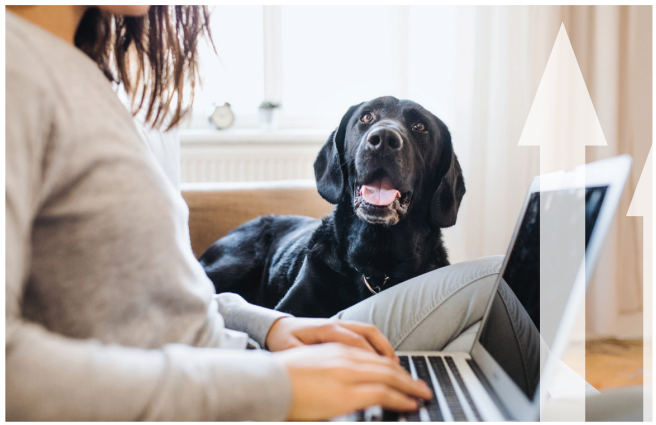
- **Isolering av dator.** När ett hot upptäcks bör den infekterade datorn kopplas bort från förbindelsen med andra delar av nätverket för att hindra att smittan sprids.

8. Behåll kontrollen över trådlösa nätverk

Vid arbete hemifrån kan även säkerhetsproblem kring användning av trådlösa nät uppstå. För distansarbetare som befinner sig i tätt bebodda områden, t.ex. lägenheter, kan varje trådlös enhet, såsom dörrens ringklocka, spelkonsoler och IoT-enheter vara möjligheter för illvilliga grannar att avlyssna trafiken. Illvilliga grannar kan missbruka faktumet att deras hus är fyllda av människor som arbetar hemifrån och där Wi-Fi utgör nästan 50 % av all IP-trafik.

Saker att ta hänsyn till kring trådlösa nät vid distansarbete:

- **Överväg att distribuera accesspunkter som certifierats enligt Trusted Wireless Environment** för att ge IT-avdelningen full insyn i klientens och nätverkets prestanda så att de på ett bättre sätt kan stödja distansarbetare.
- **Förkonfigurera accesspunkter** för enkel distribution till hemmaanvändare.



I tätt bebodda områden, t.ex. lägenheter går nästan **50 % av all IP-trafik över trådlösa nätverk**.

DÄRFÖR ÄR AFFÄRSBEREDSKAPEN VIKTIG INOM IT-SÄKERHET

Enkelt uttryckt finns det olika saker som du inte kan förutsäga. Företagsledare vet att det kommer att finnas svårigheter och oplanerade händelser längs vägen. Vad kan då du göra för att säkra din framtid? En beredskapsplan garanterar inte perfektion, men den kan ge dig verktyg som låter dig på ett säkert sätt navigera bland utmaningarna och tillhandahålla nödvändiga resurser för att säkerställa kontinuitet i verksamheten.

Idag brottas vi med coronavirusets utbrott, men nästa gång kan det vara vad som helst, och inte bara katastrofer. Stora händelser, t.ex. ett VM, kan störa hur en stad vanligtvis fungerar. Exempelvis kan också mänskliga misstag tvinga ert företag att gå över i kritiskt beredskapsläge. Alla situationer som tvingar er att snabbt anpassa er till oväntade förändringar är det ultimata beviset på hur viktigt det är att verkligen förstå er organisation och dess behov.

Varför? Därför att det visar för era anställda, kunder och intressenter att företaget kan blomstra även i oväntade och oförutsedda situationer. Ja, visst är det bra för varumärket. Men ännu viktigare är att det skapar en stark känsla av tillförlitlighet bland alla berörda. Dessutom ger det er en fantastiskt värdefull historia att berätta under många år framöver.

Varför? Därför att det visar för era anställda, kunder och intressenter att företaget kan blomstra även i oväntade och oförutsedda situationer.

CHECKLISTA FÖR IT-KONTINUITET I FÖRETAGET

Bedömning av företagets funktioner för distansarbete

Är mitt företag förberett?	Ja	Nej	Åtgärd
Har ni uppdaterat företagets policy för arbete i hemmet under de senaste 12 månaderna?			
Har du kommunicerat de policyer och förväntningar som gäller för alla medarbetare som nu arbetar hemifrån?			
Behöver ni skaffa fler telefoner/bärbara datorer så att alla anställda kommer att ha godkända enheter?			
Har ni tillräckligt med VPN-licenser för att kunna dela ut dem när de behövs?			
Har medarbetaren tillräckligt god internetanslutning för att kunna utföra sitt jobb?			
Har ni kontrollerat att era distansarbetare har tillgång till de system och plattformar som behövs för att de ska kunna utföra sitt jobb? *exempelvis molntillämpningar*			
Kan företaget tillhandahålla säkerhetsåtgärder för att undvika risker för IT-attacker vid distansarbete? *till exempel Skydd för trådlöst nätverk, VPN-anslutning, multifaktorautentisering*			
Behöver ni anpassa IT-budgeten för att leverera nödvändiga resurser?			
Behöver ni erbjuda distansutbildning till personalen om säkert arbete?			

GRATIS TJÄNSTER FÖR HJÄLP TILL SMÅ OCH MEDELSTORA FÖRETAG UNDER DE NUVARANDE EXTRAORDINÄRA HÄNDELSERNA

Våra produkter drivs med tekniken WatchGuard

WatchGuard® är en global ledare inom nätverkssäkerhet, säkra trådlösa nätverk, multifaktorautentisering och nätverksintelligens. Över 10 000 säkerhetsåterförsäljare och tjänsteleverantörer litar på företagets prisbelönta produkter för skyddet av fler än 80 000 kunder och tillhandahåller de grundläggande tekniska lösningar som behövs för att bekämpa dagens aggressiva hot.