logitech

FÖRBÄTTRAD CYBERSÄKERHET I ETT EXPANDERANDE RISKLANDSKAP

Hur säkra anslutningar mellan trådlös kringutrustning kan hjälpa till att förhindra cyberincidenter och ge anställda kontroll på den hybrida arbetsplatsen.

Den nya arbetslogiken

Innehållsförteckning

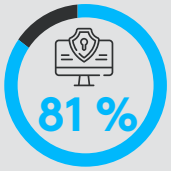
Den nya arbetslogiken: risk och verklighet

Arbetsvärlden har förändrats snabbt sedan pandemin. Medan företag inledningsvis skyndade sig att möjliggöra distansarbete, har de anställda inte bara kommit att tycka om en hybrid miljö, de arbetar till och med bättre i en sådan miljö. Idag har många organisationer fullständigt anpassat sig efter en hybrid strategi. Dock har denna övergång till mera dynamiska arbetsrutiner skapat en ny verklighet vad gäller företagssäkerhet för IT-avdelningar över hela världen. Användarna arbetar numera där det passar dem bäst, i stället för inom de skyddade begränsningarna av företagets brandvägg.

Med övergången till "den nya arbetslogiken" där traditionella skrivbordsstationer inte längre är det optimala sättet att vara produktiv, har bärbara datorer kommit att bli centrala i många människors arbetsliv. De gör det möjligt för team att vara produktiva var de än befinner sig, oavsett om det är i kollektivtrafiken, i ett café eller i hemmet. Denna utökade hotbild har varit en betydande anledning till bekymmer för IT-avdelningar och utsätter företagsenheter och nätverk för nya risker.

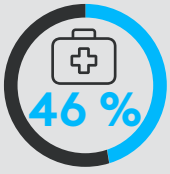
Faror som företag står inför i dagsläget

Riskerna för cyberincidenter har stigit på sistone, oavsett om man är ett företag, en offentlig tjänst, en myndighet, en utbildningsinstitution eller en individ.



Under pandemin **upplevde 81 % av alla globala organisationer ökad cybersäkerhetsrelaterad aktivitet** och 79 % drabbades av driftavbrott på grund av en cyberincident under en period med hög trafik[1].

Enligt ENISA (The European Union Agency for Cybersecurity), har antalet cyberincidenter som inriktar sig på "kritiska sektorer" fördubblats under 2020, tillsammans med en **46 % ökning vad gäller incidenter som inriktar sig på sjukhus och sjukvårdsnätverk**[2].



Kostnaderna för ett intrång har även mångdubblats. För organisationer innebär strängare dataskyddslagar, som exempelvis europeiska GDPR, att tunga böter på upp till 20 miljoner euro eller 4 % av den globala omsättningen (beroende på vad som är högst) kan läggas till de ryktesrelaterade, ekonomiska eller verksamhetsrelaterade skador som orsakas av en cyberattack.

Med en **genomsnittlig kostnad på omkring 4 miljoner euro för ett intrång**, har cybersäkerhet hamnat i det främsta rummet för organisationer inom alla sektorer. Detta bör vara något som även alla medarbetare är medvetna om, i synnerhet eftersom **95 % av alla problem med cybersäkerhet orsakas av den mänskliga faktorn**[3].

I likhet med de flesta attacker utnyttjar cyberattacker svaga punkter hos sina offer. Detta kan handla om en dåligt kodad webbplats, en anställd som är slarvig eller har onda avsikter, skadlig programvara i en e-postbilaga, en stulen enhet eller föråldrad program- eller maskinvara.

Bristande kunskaper vad gäller cybersäkerhet bland de anställda ökar också dessa risker. Genom att gå ett steg längre än standardåtgärderna för cybersäkerhet kan företagen visa reglerande organ, sina försäkringsgivare och, viktigast av allt, sina kunder att de har gjort allt i sin makt när det gäller att skydda sina system.

I denna vitbok kommer vi att titta närmare på ett exempel på hur företag, organisationer och institutioner av alla storlekar kan förbättra sitt säkerhetstänkande, oavsett om personalen arbetar på kontoret, i hemmet eller på resande fot, genom att skydda trådlösa tangentbord och möss.

En ofta förbisedd säkerhetssvaghet för företag

Med ”den nya arbetslogiken” har IT-organisationer implementerat ett stort antal nya säkerhetsåtgärder och policyer för att skydda distansarbetare.

Här ingår VPN:er, programvara för förstärkt ändpunktsäkerhet, hanteringssystem för mobila enheter, flerfaktorautentisering, med mera. Men även med dessa skyddsåtgärder införda, finns det fortfarande en källa för svagheter och värdefulla data för hackare och det handlar om informationen som överförs mellan trådlösa enheter och själva datorn.

Hur kan du säkra kringutrustning och skydda ditt företag bättre?

IT-avdelningarna måste se till att anslutningarna som används av trådlösa möss och tangentbord är så säkra som möjligt, för att undvika att de äventyras. För dem som har begränsade resurser, i synnerhet små och medelstora företag, är dessa åtgärder av avgörande betydelse för att förhindra obehörig åtkomst till data och system.

Det första steget är att se till att alla enheter är uppdaterade vad gäller firmware och att anslutningarna de upprättar är krypterade.

För enheter som utnyttjar *Bluetooth*®, bör anslutningen använda sig av Security Mode 1, Level 4 (Secure Connections Only-läge), som uppfyller kraven för FIPS (Federal Information Processing Standards). För enheter som ansluts via en USB-dongel, bör man leta efter en anti-rollback-funktion (förhindrande av återställning) för firmware-uppgraderingar (DFU:er) som är säkerhetsbaserade.

Detta hjälper till att säkerställa att kritiska säkerhetskorrigeringar inte tas bort oavsiktligt medan rollbacks av ej säkerhetsrelaterade uppdateringar tillåts.

Hur säker är din kringutrustning?

- Uppdaterar du enheternas firmware regelbundet?
- Använder trådlösa tangentbord och möss sig enbart av Secure Connections Only-läget?
- Kan du förhindra enheter som är anslutna till en USB-dongel från att återställas till tidigare firmwareversioner?

Logi Bolt: en säker lösning

Sättet som företag tänker kring trådlös kringutrustning för datorer har utvecklats i takt med att säkerhetsriskerna ökar i en hybrid värld. Idag fokuserar företagen primärt på följande när det gäller kringutrustning:

- **Säkerhet**
- **Prestanda i miljöer med hård belastning**
- **Kompatibilitet över flera plattformar**

Det är därför som Logitech har tagit fram ett egenutvecklat protokoll med namnet Logi Bolt, baserat på *Bluetooth*® Low Energy (BLE), som implementerar säkerhetsfunktioner för att förhindra man-in-the-middle (MITM)-attacker och undvika tjuvlyssnande och injektioner. Logi Bolts teknik är fullständigt krypterad och FIPS-godkänd. Detta säkerställer att en trådlös Logi Bolt-produkt och Logi Bolt-USB-mottagaren endast kan kommunicera med varandra.

Med Logi Bolt tillhandahåller Logitech förbättrad säkerhet på företagsnivå och en robust signal, även i trådlösa miljöer med hård belastning. Med sin kompatibilitet med alla större operativsystem och plattformar, är det även enkelt att driftsätta och hantera för både stora och små IT-avdelningar.

Säker anslutning

Logi Bolt säkerställer kommunikation mellan trådlösa möss och tangentbord. USB-mottagaren är alltid krypterad och använder sig av Authenticated Low Energy Secure Connections (LESC)-krypterad sammankoppling.

Skyddad sammankoppling

Logi Bolt-USB-mottagare tillämpar endast Secure Connection Only-läget, där sammankopplingen kräver att de två enheterna är autentiserade och att länken är krypterad.

Enkel och säker hantering

Logi Bolt erbjuder säkerhetsåtgärder med självservice som fortfarande möjliggör centraliserad översikt, inklusive aviseringar när sammankoppling för en ny enhet begärs.

Förbättrad säkerhet bör inte innebära att man måste kompromissa när det gäller valmöjligheter, komfort eller produktivitet

Den bärbara datorn är favoritverktyget i dagsläget, i synnerhet för distansarbetare. Men även om de är perfekta vad gäller rörlighet, är de kompakta tangentborden och styrplattorna inte idealiska ur ett ergonomiskt perspektiv eller för produktivt arbete under längre tidsperioder.

Trådlösa möss och tangentbord erbjuder en flexibel lösning som ger anställda friheten att placera sina anslutna enheter efter egen bekvämlighet, utan att göra arbetsytan för trång.

Genom att använda Logitech for Business-lösningar tillsammans med Logi Bolt kan anställda och deras organisationer dra nytta av det bästa från två världar: säkra anslutningar och ett urval av kringutrustning som passar deras behov.

Logitech for Business-lösningar med Logi Bolt

MX Master Series for Business

Oöverträffad precision och prestanda, i kombination med Logi Bolt-teknik, idealiskt för analytiker, kreatörer, kodare och alla med mycket specialiserade arbetsflödesbehov.

MX KEYS COMBO FOR BUSINESS

Kombinationen MX Keys for Business och MX Master 3S for Business med stöd för handflatan är den ultimata mus- och tangentbordskombinationen för hög produktivitet.

MX KEYS FOR BUSINESS

Öka produktiviteten för kodare, analytiker och kreatörer som behöver stabilitet, precision och kraft för att höja sina arbetsprestationer.

MX MASTER 3S

MX Master 3S for Business är vår stilbildande mus, nu ännu bättre med Quiet Click-teknik som minskar klickljuden med 90 %. Den fungerar på alla ytor, till och med glas, med en 8K DPI-sensor med anpassningsbar känslighet.

MX KEYS MINI COMBO FOR BUSINESS

MX Keys Mini Combo for Business. En kompakt, högpresterande mus och tangentbord som frigör mer arbetsyta för ökad produktivitet.

MX KEYS MINI FOR BUSINESS

Med avancerad funktionalitet i en elegant minimalistisk design är MX Keys Mini for Business perfekt för dem som behöver mer arbetsyta – särskilt kreatörer med ett krävande arbetsflöde.

MX ANYWHERE 3 FOR BUSINESS

Ultimat mångsidighet möter anmärkningsvärd prestanda Upptäck den kompakta musen som har tagits fram för mobilt arbete – från hemmakontoret till caféet och flygplatsloungen.

MX MASTER 3 FOR BUSINESS

Oöverträffad precision och prestanda för analytiker, kreatörer, kodare och alla med mycket specialiserade arbetsflödesbehov.

Ergo Series for Business

Möss och tangentbord som är vetenskapligt framtagna för att främja en mer naturlig hållning och minskad muskelbelastning.

ERGO K860 FOR BUSINESS

Ge användarna frihet att fokusera med ett vetenskapsdrivet tangentbord som främjar en mera avslappnad och naturlig skrivupplevelse. Den är framtagen för timtals bekväm användning.

LIFT FOR BUSINESS

Lift for Business, som är godkänd av ergonomer, har rätt storlek för alla händer, både vänster- och högerhänta, förbättrar hållningen och minskar muskelutmattningen i underarmen.

ERGO M575 FOR BUSINESS

Med vetenskapsdriven design och enkel tumstyrning är denna trådlösa trackballmus framtagen för att minska handrörelserna och hålla handen och armen avslappnade för timmar av bekvämt arbete.

Signature Series for Business

Förbättra produktiviteten, komforten och den övergripande medarbetarupplevelsen genom att tillhandahålla Logitech Signature for Business-lösningar.

SIGNATURE MK650 COMBO FOR BUSINESS

Den trådlösa Signature MK650 for Business-musen är framtagen för komfort och ökar produktiviteten med 50 % och arbetshastigheten med 30 % jämfört med en styrplatta på en bärbar dator.

SIGNATURE M650 FOR BUSINESS

Den trådlösa Signature M650 for Business-musen är framtagen för komfort och ökar produktiviteten med 50 % och arbetshastigheten med 30 % jämfört med en styrplatta på en bärbar dator.

SIGNATURE M650 L FOR BUSINESS

Vi rekommenderar Signature M650 för små till medelstora händer och Signature M650L för större händer.

Flera enheter

Genom att använda Logitech for Business-lösningar med Logi Bolt kan de anställda arbeta snabbare och mera produktivt var de än befinner sig, samtidigt som säkerheten upprätthålls.

En enskild Logi Bolt-mottagare kan sammankoppla upp till sex Logi Bolt-enheter med tre aktiva anslutningar, vilket gör det särskilt praktiskt för anställda som använder olika enheter på kontoret, i hemmet och på resande fot.

Med Logi Bolt-mottagaren ansluten till den bärbara datorn kan man använda olika slags kringutrustningar med Logi Bolt på ett säkert sätt, var man än befinner sig.

Starkare signal, omfattande kompatibilitet

Utöver säkerhet är anslutningskvalitet och kompatibilitet viktiga överväganden för organisationer när det gäller val av kringutrustning. Logi Bolt är utvecklat för tillförlitliga anslutningar, även i trådlösa miljöer med mycket störningar från WiFi-anslutningspunkter eller närliggande trådlösa enheter.

Logi Bolts USB-mottagare erbjuder en stark, tillförlitlig, störningsfri anslutning på upp till 10 meter, i många fall med upp till åtta gånger lägre latens än andra vanligt förekommande mottagare i företagsmiljöer med hög trafik.

Dessutom fungerar Logi Bolt,i princip, med samtliga operativsystem och plattformar. Faktum är att Logi Bolt-enheter är mera allmänt kompatibla än de flesta ledande märken för kringutrustning på marknaden.

Fler valmöjligheter utan kompromisser

Det finns en Logitech for Business-lösning med Logi Bolt för varje användarbehov, oavsett om man är en upptagen användare med ett krävande arbetsflöde, behöver enkelhet och förbättrad produktivitet eller behöver ökad komfort med hjälp av ergonomi.

Logi Bolt-teknologi återfinns inom Ergo-, Signature- och MX-sortimenten för Logitech for Business tangentbord och möss, vilket säkerställer att användarna kan arbeta på ett sätt som passar dem, utan att kompromissa med säkerheten.

Förbättrad säkerhet för en föränderlig arbetsvärld

I dagens ”nya arbetslogik” med ökande cyberrisker, måste företag identifiera sårbarheter inom organisationens samtliga områden. Logitech for Business-kringutrustning med Logi Bolt förser organisationer med fler valmöjligheter när det gäller att skydda sin verksamhet och ge sina anställda handlingsfrihet. Det gör dem utöver att leverera en kraftfull och tillförlitlig anslutning och bred kompatibilitet.

Kringutrustning med Logi Bolt förser företag med alternativet att snabbt öka säkerheten efter behov, utan att kompromissa med användarupplevelsen, oavsett om det utgör en del av en enhetsuppdatering eller en justering av en säkerhetspolicy. I takt med att Logi Bolt läggs till på ännu fler enheter i sin ”for business”-portfölj för kringutrustning, arbetar Logitech intensivt för att ge organisationer och slutanvändare fördelen av valfrihet och flexibilitet, samt ökad produktivitet och bättre skydd.

Ta reda på mer om Logi Bolt och Logitech for Business-lösningar

Kontakta Logitechs försäljningsavdelning

Källor

1. https://www.businesswire.com/news/home/20211108005775/en/Cyber-Threats-Have-Increased-81-Since-Global-Pandemic
2. https://edition.cnn.com/2021/06/10/tech/europe-cyberattacks-ransomware-cmd-intl/index.html
3. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf