Läs mer på **tillvaxtsverige.se**

Samhällssäkerhet

Åsa Ahl

Stärkt säkerhets-skydd gynnar hela Sverige

Rote Consulting
Läs om Gabor Nagys tankar om säkerhetsläget
Sida 2

Sectra
Cybersäkerhet – central del av totalförsvaret
Sida 4

I DETTA NUMMER

Projektledare: **Mimmi Fouchenette** (mimmi.fouchenette@mediaplanet.com) Verkställande direktör: **Axel Landberg** Redaktionschef: **Tim Sobek** Affärsutvecklare: **Arvid Olofsson** Designer: **Daniel Petersson** Distribution: **Dagens Industri, 27-12-2021** Tryckeri: **V-Tab** Mediaplanet kontaktinformation: E-post: **tim.sobek@mediaplanet.com** Omslagsfoto: **Säkerhetspolisen**

facebook.com/MediaplanetSverige

@Mediaplanetsweden

Återvinn gärna tidningen

Mimmi Fouchenette, projektledare:

Med den här satsningen vill vi belysa vilka utmaningar svenskt samhälle står inför idag och hur dessa ska hanteras. Med de fokusområden som lyfts här kan det ge en överblick kring Sveriges samhällssäkerhet. Jag önskar dig en trevlig läsning!

LEDARE

Att fortsätta i utpekad riktning

Det säkerhetspolitiska läget globalt och i närområdet utmanar vårt samhälle. Utvecklingen av vår krisberedskap och vårt totalförsvar för att möta utmaningarna kan dess bättre skönjas och har en av regeringen utpekad ritning. Det är av stor vikt att riktningen nu följs så att strukturer som succesivt byggs upp skapar en ökad motståndskraft mot de hot vi står inför. Ett målinriktat arbete genomförs i form av inte bara utredningar, utan även inom och mellan myndigheter, organisationer och företag.

Text Gabor Nagy

Nya strukturer
Förslag på en strukturell geografisk indelning av Sverige finns, så även ett förslag på beredskapssektorer med ingående myndigheter där förutsättningar för att skapa lägesbilder, koordinera och att göra prioriteringar förbättras. Arbete med att anlysera och föreslå en funktion för nationell samordning av vår försörjningsberedskap med förslag på ansvar mellan det offentliga och näringslivet har påbörjats. Näringslivet utgör merparten av samhällets resurser. Det finns en adminstrativ beredskap för inordnande av dessa resurser vid höjd beredskap, men det är väsentligt att en funktionalitet kopplad till dagens förutsättningar klarläggs.

Planeringsförutsättningar
Försvarsmakten och Myndigheten för samhällsskydd och beredskap har enligt ett regeringsuppdrag utformat en handlingsplan för utvecklingen av Sveriges totalförsvar – ”Handlingskraft”. Här ges planeringsförutsättningar av det förväntade hotet och vad detta hot i praktiken innebär. ”Handlingskraft” innehåller även fokusområden som efter analys av nuvarande förmågor är de som initalt ska förbättras för att minska våra sårbarheter, vilket naturligtvis är av stor vikt. Om inte riskerar vi att bygga ett system och ett totalförsvar med svaga länkar som ger en antagonist uppenbara sårbarheter att angripa.

Det flerdimensionella hotet
Ett angrepp mot Sverige kommer inte endast att utgöras av militära maktmedel, utan kommer att bestå av assymetriska angrepp mot våra sårbarheter. Du, ditt företag, organisation eller myndighet är en del av Sveriges totalförsvar. Genom att förbättra identifierade och beslutade fokusområden bidrar du till vårt försvar och till den helhet som bygger på lojalitet och ansvarstagande från var och en av oss.

> Ett angrepp mot Sverige kommer inte endast att utgöras av militära maktmedel, utan kommer att bestå av assymetriska angrepp mot våra sårbarheter. Du, ditt företag, organisation eller myndighet är en del av Sveriges totalförsvar.
>
> **Gabor Nagy**
> Totalförsvar
> Rote Consulting AB

Det gemensamma ansvaret
Vår gemensamma säkerhet bygger på ett personligt ansvar att bidra och detta är en förutsättning också för din personliga säkerhet vid en kris eller krig.

Att fortsätta i den utpekade riktningen är en del av att bidra och en förutsättning för att vi, i Sverige tillsammans, ska lyckas med att skapa det samhälle och totalförsvar som krävs för att bibehålla vår säkerhet, självständighet och frihet.

FOTO: GETTY IMAGES

FOTO: GETTY IMAGES

Hur man bygger ett **motståndskraftigt företag i tuffa tider**

Inbyggd motståndskraft kan vara skillnaden mellan framgång eller konkurs vid katastrofer. Hur ska man kunna förbereda sig för det oförutsedda? Ett sätt är att använda ett perspektiv som spänner över hela organisationen, i kombination med programvara med stöd för att utvärdera hot och som automatiserar snabb informationsspridning.

Text Anders Edström Frejman

Strömavbrott, förödande bränder, cyberattacker som slår mot IT-system eller en terrorattack.

När organisationer traditionellt försöker bygga in motståndskraft mot katastrofer eller andra oönskade händelser så fokuserar man ofta på att ta fram olika scenarios. Sedan utvecklas handlingsplaner för varje händelse.

Det grundläggande problemet med ett sådant angreppssätt är att en organisation riskerar att stå oförberedd för det oförutsedda, säger Tracy Reinhold, Chief Security Officer på Everbridge.

9/11, finanskrisen och Covid-19 är bara tre exempel på händelser som påverkade miljoner organisationer, små som stora, från golvet upp till styrelserummen, från privatpersoner till hela nationer.

Den gemensamma nämnaren är att de var näst intill omöjliga att förutsäga, liksom de långsiktiga konsekvenserna.

Undvik dolda växande hot

Detta sätter fingret på nödvändigheten av ett perspektiv som spänner över hela organisationen, för att uppnå varaktig uthållighet, skydda människoliv, företagets tillgångar, kundrelationer och minimera tiden tillbaka till normaltillståndet.

– I traditionella organisationer har man olika silos för fysisk säkerhet och cybersäkerhet. Problemet är att hot – bildligt talat – kan gömma sig och växa mittemellan, speciellt i en digital värld där traditionella gränser mellan ansvarsområdden suddas ut.

Dessa gap behöver stängas och nya hot måste hanteras. Till exempel så kallad ”social engineering” som innebär att organisationer attackeras med en stor bredd av sofistikerade metoder från cyberkriminella.

Ett holistiskt arbetssätt

Tracy Reinhold, med en bakgrund från den finansiella sektorn och dessförinnan 20 år på FBI, förespråkar ett holistiskt synsätt på krishantering för att uppnå motståndskraft.

– Everbridges programvarulösning för att stödja företag vid kritiska händelser - Critical Event Management, CEM - förser organisationer med information om kritiska händelser för att stödja arbetet med personsäkerhet och hjälpa till att upprätthålla verksamheten, säger han.

Grundkonceptet bakom CEM är att - i händelse av en kritisk händelse - kunna hålla personal och tillgångar säkra samtidigt som verksamheten hålls rullande. Detta kan uppnås genom automatiserade processer, informationsinhämtning från partners och företagsinterna källor. CEM hjälper användare att utvärdera risker och ta välgrundade snabba beslut.

Automation som räddar liv

CEM-lösningen kan till exempel hjälpa organisationer att snabbt få fram information om anställdas geografiska position och skador på tillgångar. Processer som stödjer detta tas fram i förväg genom att skapa företagsspecifika mallar för att kunna leverera snabb, korrekt, relevant information som anpassas för mottagaren. Vissa rutiner kan automatiseras fullt ut när tiden är allt för att rädda liv.

– Att leverera konsekvent och korrekt information utanför organisationen är dessutom avgörande för att bygga förtroende, skydda ryktet och aktievärdet.

Tracy Reinhold ser att företagsledningar, styrelser och ägare börjar förstå värdet av att bygga motståndskraftiga organisationer.

– Traditionellt sågs området säkerhet enbart som en kostnad. Denna förståelse för motståndskraft i ett brett perspektiv betraktas numera som en tillgång. Jag kan inte annat än hålla med.

FOTO: EVERBRIDGE

Tracy Reinhold
Chief Security Officer
Everbridge

Vill du veta mer om Everbridge?

Besök

Everbridge.com

Denna artikel är i samarbete med **Everbridge**

Denna artikel är **i samarbete med Sectra.**

SECTRA

Cybersäkerhet – central del av totalförsvaret

Cybersäkerhet är en viktig del av totalförsvaret på grund av samhällets beroende av digitala tjänster. Men säkerhetslösningar får inte komma i vägen för den dagliga verksamheten. Då finns risk att anställda tvingas kompromissa med säkerheten.

Text Anders Edström

Digitaliseringen har på ett tiotal år både effektiviserat offentliga verksamheter och i grunden förändrat hur vi arbetar och lever våra liv. För det mesta till det bättre genom att vardagen har förenklats, till exempel via digitala tjänster för handel, banktjänster, sjukanmälan och möjligheter till distansarbete. Men digitaliseringen har också medfört tydliga risker.

– Cyberattacken på COOPs och Apotekets underleverantör som helt stängde ned deras kassor är ett exempel som påverkade många privatpersoner. Det visar tydligt hur beroende samhället är av digitala tjänster, säger Lasse Larsson på Sectra Communications.

Internationell trend

Cyberattacker – av kriminella och i vissa fall statsunderstödda organisationer – har tydligt ökat i omfattning och är ett internationellt fenomen. Målen och syftena kan vara hela skalan från ekonomiska utpressningsförsök på enskilda individer, företag eller offentlig verksamhet till att destabilisera hela nationer. Det senare till exempel genom att attackera infrastruktur för energiförsörjning. Under 2021 attackerades bland annat danska vindturbintillverkaren Vestas och amerikanska Colonial Pipeline.

– Så kallad ransomware har även blivit ”populär” vid attacker emot vårdsektorn. Ett sjukhus till exempel är en kritisk funktion i samhället, där det konkret handlar om mänskliga liv och är en verksamhet som bara måste fungera, därmed blir det ett attraktivt mål för en angripare.

Viktig del i totalförsvaret

Lasse Larsson – som bland annat arbetar med Försvarsmakten och aktörer inom civilförsvaret – menar att exemplen ovan visar att cybersäkerhet behöver ses i ett större perspektiv. Som en del av totalförsvaret.

– Sectra har bland annat NATO, EU och nationella säkerhetstjänster som kunder. Vi tillhandahåller säkra telefoner, säker och godkänd VPN-teknologi, krypton och andra lösningar som inte ens kvantdatorer ska kunna knäcka. Men cybersäkerhet är mycket mer än säkerhetslösningar och AI som upptäcker avvikande trafikmönster. Den mänskliga faktorn är en riskfaktor i sig. Jag brukar säga att det måste vara lätt att göra rätt.

Farliga målkonflikter

Cybersäkerhet måste vara inarbetad som en naturlig del i verksamheten – inte vara ett krångligt tillägg som stör. Det får aldrig finnas en målkonflikt mellan säkerhet och att uppnå affärsplaner. Om så är fallet kommer verkligheten tvinga anställda att kompromissa och säkerheten äventyras. Lasse tar ett praktiskt exempel.

– I mitt arbete kan jag, av säkerhetsskäl, bara ha appar installerade på min tjänstetelefon som vi vet är säkra. Rent konkret leder detta till att jag i vissa undantagsfall behöver ha en separat telefon för till exempel lokala parkeringsappar. Organisationer behöver på liknande sätt göra vissa ställningstaganden av säkerhetsskäl.

Han berättar att verksamheter som lyckas med säkerhetsarbetet är de som kontinuerligt arbetar med säkerhetsfrågor och som hela tiden implementerar säkerheten in i den dagliga verksamheten. Bland annat med återkommande utbildning och stickprov där man till exempel testar anställdas vaksamhet mot falska mejl.

– Det är med säkerhetsarbete som med trafikplanering. När du bygger bort en flaskhals på ett ställe får du trängsel på ett annat. När man arbetar kontinuerligt med att stärka cybersäkerheten flyttas den svagaste punkten i kedjan. Vi hjälper våra kunder på den resan.

FOTO: SECTRA

Lasse Larsson
Chef för Kritisk Infrastruktur
Sectra Communications

Cybersäkerhet är inte ett självändamål i sig, utan en förutsättning för överlevnad

ILLUSTRATION: SHUTTERSTOCK

Text Janne Haldesten

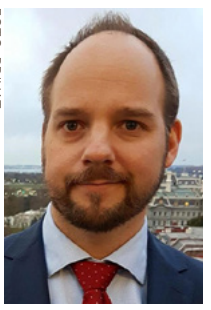
Den tekniska utvecklingen och digitaliseringen går allt snabbare, där säkerheten hamnat på efterkälken. Graden av digitalisering har också inneburit att flertalet IT-system inte längre bara är ett stöd för verksamheten, utan har blivit en förutsättning för att verksamheten överhuvudtaget ska fungera, oavsett om det rör sig om myndigheter eller företag. Dessa beroenden skapar samtidigt en mer övergripande säkerhetsutmaning, där allt fler system kopplas samman, där angrepp mot ett eller några system kan få kaskadeffekter mot desto fler, och där detta ytterst kan komma att hota Sveriges säkerhet och våra samhällskritiska funktioner. Sammantaget har denna utveckling inneburit att organisationer inom både offentlig liksom privat sektor är sårbara för olika typer av cyberhot, alltifrån statliga hotaktörer till cyberbrottslighet.

Vägen framåt

Då en övervägande del av den samhällskritiska infrastrukturen drivs av privata företag så måste samverkan och samordning mellan offentlig och privat sektor bli bättre nationellt, något som är av yttersta vikt för det fortsatta totalförsvarsarbetet, liksom för bekämpningen av cyberbrottslighet.

Vidare måste dagens ledningsgrupper förstå grundläggande IT-säkerhet, då det inte räcker med ett verkanslöst ledningssystem för informationssäkerhet. Ett cyberangrepp tar inte hänsyn till hur välskriven en policy är, utan snarare hur välimplementerad den är i praktiken.

FOTO: PRIVAT



Janne Haldesten
Cyberspecialist

Erfarenhetsmässigt kan det konstateras att det är de "enkla" sakerna som många gånger falerar, såsom att hålla ordning på vad som finns i den egna miljön; det är svårt att skydda det man inte vet att man har, där ett icke-underhållet system kan skapa en inbrytningspunkt för en angripare, där denne sedan rör sig vidare inne i målmiljön i jakt på "kronjuvelerna". Därav är även segmentering, detekteringsförmåga och behörighetshantering av stor vikt.

Avslutningsvis, enskilda organisationer, eller vi som samhälle, har inte råd att fortsätta som vi gjort. Vi kan helt enkelt bättre!

> *Ett cyberangrepp tar inte hänsyn till hur välskriven en policy är*

Denna artikel är **i samarbete med Svenska Fallskärmsförbundet.**

Svenska Fallskärmsförbundet

Eufori och samhällstjänst

Fallskärmshoppning innebär en stor gemenskap och glädje för många, men kan i förlängningen också växa fram som en samhällsnytta i krisberedskap. Kombinationen kan bli väldigt nyttig i framtiden.

FOTO: SVENSKA FALLSKÄRMSFÖRBUNDET

Sven Mörtberg
Riksinstruktör
Svenska Fallskärmsförbundet

FOTO: VIKTOR ENGBERG

Text Fredrik Söderlund

Det finns ingen stereotyp hoppare, utan fallskärmshoppning lockar många olika åldrar och människor med flera olika kompetenser, säger Sven Mörtberg som är Riksinstruktör och verksamhetsansvarig för all civil fallskärmshoppning i Sverige.

– De som söker vill ofta göra någonting utöver det vanliga och det brukar hänga ihop med att man gillar utmaningar och att pusha sig själv. Vi önskar att fler ska få uppleva den eufori som fallskärmshoppning innebär. Den ger också möjlighet till personlig utveckling på många olika sätt.

En stor gemenskap

Själva fallskärmshoppningen är en fantastisk upplevelse och det växer fram en stor gemenskap och glädje bland hoppare, menar Sven Mörtberg.

– Det är såklart nervöst i början, men oftast övergår det i fokuserad anspänning. I ett senare stadie kan du även hoppa tillsammans med andra. Hoppningen blir en livsstil som knyter många starka band mellan utövarna

Stöd till Försvarsmakten

SFF är också en frivillig kompetensorganisation som spelar en viktig roll för Sveriges kris- och krigsberedskap. En uppgift är bland annat att stödja Försvarsmakten med att vidareutbilda militär personal i fallskärmshoppning.

– Vi kan med vår särskilda kompetens komplettera den befintliga krisberedskapen. Som ett exempel kan vi släppa ner samhällsutrustning, medicin eller liknande med fallskärm. Vi har många välutbildade instruktörer som kan ta en ledarroll eller vara en tillfällig insats.

Ett viktigt samarbete med MSB

På senare år har SFF även utvecklat ett samarbete med Myndigheten för Samhällsskydd och Beredskap (MSB).

– Vi använder hoppning som både nöje och idrott, men är också en del av totalförsvaret. SFF är en frivillig försvarsorganisation som kan verka i ett försvarssyfte med en unik kompetens.

FRA

FÖR DIN TRYGGHET.
FÖR VÅR DEMOKRATI.
VARJE DAG.
ÅRET OM.

Vill du också bli en av de bästa?
Läs mer på fra.se/jobb

ÅSA AHL

Stärkt säkerhetsskydd gynnar hela Sverige

Det finns ständigt krafter som vill försvaga Sveriges funktionalitet eller stjäla våra industri- och forskningshemligheter. En gedigen säkerhetsskyddsanalys på företag och institutioner är det första steget mot en ökad säkerhet som gynnar alla. Det menar Åsa Ahl, säkerhetsskyddsexpert på Säkerhetspolisen.

Text Christian von Essen

En stor del av Sveriges framgångar vilar på ett fundament av tillit, öppenhet och frihet. Men samma mekanismer som främjar entreprenörskap, forskning och innovationskraft riskerar också att göra oss sårbara.

Från Säkerhetspolisens perspektiv är det framförallt tre nationer som skulle kunna ha tillräckligt med såväl egenintresse som resurser för att vilja bedriva spionage eller annat påverkansarbete för att försvaga det svenska samhället: Iran, Ryssland och Kina.

Åsa Ahl är säkerhetsskyddsexpert på Säkerhetspolisen (Säpo). Hon menar att den utländska aktiviteten har ökat under de senaste fem åren.

– Framförallt ser vi att fler typer av verksamhetsutövare påverkas av de säkerhetshotande aktiviteterna från främmande makt. Tidigare var det främst militära syften som låg bakom, men i dag kan såväl forskningsinstitut och universitet som privata företag ligga i riskzonen.

Säkerhetsskyddsanalys krävs

I säkerhetsskyddslagen och säkerhetsskyddslagstiftningen stipuleras hur dessa verksamheter bör agera för att upprätta och stärka sitt säkerhetsskydd. Sedan 1 april 2019 omfattar lagen alla som bedriver någon form av säkerhetskänslig verksamhet, och 1 december 2021 stärktes tillsynsstrukturen kring lagstiftningen ytterligare.

– Globaliseringen, teknikutvecklingen och digitaliseringen har ökat sårbarheten i samhället. När känsliga uppgifter placeras i olika molntjänster blir de ännu svårare att skydda. Gapet mellan hot och sårbarhet har ökat, och därför måste vi alla samarbeta för att stärka skyddet, säger Åsa Ahl.

Men hur vet man om verksamheten omfattas av säkerhetsskyddslagstiftningen från början? Svaret kommer i regel av en intern säkerhetsskyddsanalys. Säkerhetspolisen tillsammans med Försvarsmakten utövar tillsyn för myndigheter som bedriver säkerhetskänslig verksamhet.

– Om det råder minsta osäkerhet kring de här frågorna är det förmodligen dags att genomföra en säkerhetsskyddsanalys. Och då ska det inte hamna på en ensam säkerhetsansvarig, utan det måste vara ett teamarbete som är förankrat från högsta ledningen. Först när analysen är på plats kan man gå vidare till en handlingsplan med konkreta åtgärder.

Tre skyddskomponenter

Säkerhetsskyddet omfattar tre viktiga skyddsåtgärder för verksamheten. Personalsäkerhet innebär utbildning och säkerhetsprövning av personal.

Säkerhetsprövning innebär bland annat att förebygga och hantera värvningsförsök från främmande makt för att få ut känslig information. Fysisk säkerhet kan handla om att förhindra eller försvåra intrång i verksamheten genom lås, larm och kameraövervakning. Informationssäkerhet är IT-systemens skydd, med brandväggar, behörigheter

FOTO: SÄKERHETSPOLISEN

Åsa Ahl
Säkerhetsskyddsexpert
Säkerhetspolisen

> Globaliseringen, teknikutvecklingen och digitaliseringen har ökat sårbarheten i samhället. När känsliga uppgifter placeras i olika molntjänster blir de ännu svårare att skydda. Gapet mellan hot och sårbarhet har ökat, och därför måste vi alla samarbeta för att stärka skyddet.

och lösenord.

Åsa Ahl poängterar att den röda tråden mellan säkerhetsskyddets tre delar är tydlig: människan är den svaga länken. Och med en ökning av aktiviteter inom så kallad social ingenjörskonst blir den viktigaste åtgärden därmed att höja kunskap och kompetens internt i organisationerna.

– Vi behöver öka utbildningsnivån på bred front, och jag menar att man måste börja i toppen av organisationerna för att sätta rätt typer av rutiner och riktlinjer. Samtidigt kanske det inte är hela verksamheten som omfattas av säkerhetsskyddet – det kan exempelvis vara en enhet som specifikt sysslar med forskning, utveckling eller hantering av stora mängder data. Då är det framförallt den delen som måste skyddas.

Även om man som verksamhetsutövare kommer fram till att det man gör inte omfattas av lagstiftningen kring säkerhetsskydd, finns det en poäng med att genomföra genomlysningen och vidta åtgärder.

– Det finns en stor risk i att inte arbeta proaktivt med säkerhetsskyddet. Omfattas du av lagstiftningen riskerar du från 1 december 2021 sanktioner och viten om skyddet inte är tillräckligt. Om du inte omfattas av säkerhetsskyddslagen är det ändå en god investering inför framtiden, avslutar Åsa Ahl. ■

FAKTA

Säkerhetsskyddslagen omfattar alla som bedriver ”säkerhetskänslig verksamhet som är av betydelse för Sveriges säkerhet eller som Sverige har förbundit sig att skydda genom internationella åtaganden”.

På Säkerhetspolisens hemsida finns vägledningar och riktlinjer som man kan använda sig av för att genomföra en säkerhetsskyddsanalys inom sin verksamhet.

Läs mer på
www.sakerhetspolisen.se/sakerhetsskydd.html

FOTO: SHUTTERSTOCK/WUTZKOHPHOTO

Säkerhetsprövningsintervjuer är **en vinst för företag**

Säkerhetsprövningsintervjuer är mer än bara en **bakgrundskontroll**. De kan ge bidra till ett **bättre säkerhetstänk** för både befintlig och ny personal. Dessutom kan de **hjälpa företagen** att ta bättre beslut **inför framtiden**.

Text Fredrik Söderlund

Denna artikel är **i samarbete med Recway.**

FOTO: ENGSTREAM

Zanko Dasko
Grundare
Recway

Säkerhetsförslagen skärptes från och med den 1 december. Det kommer ställas högre krav på organisationer och både inom privat- och offentlig sektor, att genomföra säkerhetsprövningar.

–Med hjälp av säkerhetsprövningsintervjuer kan man förebygga säkerhetsrisker och skapa förutsättningar för en bättre och mer harmonisk verksamhet där tillit finns i centrum.

Flera olika frågeområden

Under en säkerhetsintervju går man igenom cirka 15 olika frågeområden för att identifiera exempelvis sårbarhet, lojalitet och pålitligheten hos en person.

–Det kan vara informationen som du fått via grundutredningen, såsom aktiviteter, hur synlig du är på sociala medier, betalningsanmärkningar, böter och om du har begått något brott, säger Zanko Dasko.

Företagen tycker ofta att det räcker med en bakgrundskontroll, men då får man bara fram rådata kring personen.

–Vid en bakgrundskontroll kan du till exempel inte få reda på om en person har ett spelmissbruk, vilket såklart kan vara en risk för företaget i förlängningen. I och med samtal och säkerhetskontroll kan du få reda på saker som en vanlig bakgrundskontroll missar.

Sårbarhet kring lojalitet

En utmaning idag är att aktörer och företag gör sina egna säkerhetsprövningsintervjuer. Det innebär att företagets kunder inte kan kräva vem som ska göra intervjun, utan bara att den ska genomföras.

–Det finns mycket som personer inte vill prata om med sin chef vid ett första samtal. Exempelvis sin ekonomiska situation och sitt närmaste umgänge. Får du däremot träffa någon utomstående vid ett tillfälle, så tror jag inte att det är samma utmaning att vara öppen, menar Zanko Dasko.

> Det kommer ställas högre krav på organisationer och både inom privat- och offentlig sektor att genomföra säkerhetsprövningar.

Naturlig del av rekryteringsprocessen

Zanko Dasko tror att det kommer behövas fler säkerhetsanalyser- och prövningar hos alla typer av företag och inte bara de största i framtiden.

–Det kommer bli en naturlig del av rekryteringsprocessen, både vid nya rekryteringar och med befintlig personal. Det händer mycket i en persons liv på några år, och att få kännedom kring de förändringarna kan vara väldigt viktigt både för företaget och de anställda.

Digitalt ID blir globalt teknologiskt genombrott för blockchain- och AI-bolaget BlueBarricade

Mikael Bramstedt och BlueBarricade är redo för miljardexpansion i och med skapande av PurpleTokenID.

FOTO: TOM GOREN

Mikael Bramstedt

Med hjälp av BlueBarricade-teknologi, samutvecklad med IBM globalt, utvecklas en banbrytande digital identifieringshandling. Med tokenisering skapas en unik identitet, PurpleTokenID. Ett globalt ”Bank-ID” om man så vill, men med skillnaden att det används i en digital e-wallet inom många olika områden, såsom banktransaktioner, varor, tjänster, logistikkedjor, företagsprocesser och digitala tillgångar för hela världens befolkning. Nu är IT-arkitekten, entreprenören och innovatören Mikael Bramstedt redo för miljardexpansion med sitt svenska Fintech-team.

Samtidigt har moderskeppet BlueBarricade Blockchain & AI Technology AB emitterat 487 000 nya aktier till 20,50 EUR per aktie.

Mikael Bramstedt har tidigare brutit ny mark med bland annat den populära Swish-appen, grundandet av Netgiro som såldes till Digital River Inc. (NASDAQ:DRIV), samt lanserat en banbrytande blockchainprodukt på IBM-plattform som i dokumenterade testresultat klarat upp till blixtsnabba 1400 transaktioner per sekund. Han har över 35 års erfarenhet av banksystem och kreditkortsbolag i stordatorer i samarbete med IBM.

Redo för miljardexpansion med svenskt Fintech-team

Den nya bolagsskapelsen har kapacitet att bli nästa miljardbolag, då marknaden är oändlig för PurpleTokenID med tillhörande e-wallet. Innovationen bygger på befintlig infrastruktur i IBM Mainframe som redan används av 95 procent av världens banker, finansinstitut och kreditkortsutgivare. PurpleTokenID kombinerar BlueBarricades blockchainprodukt 1400TPS med IBM:s globala säkerhetssystem. PurpleTokenID kommer att vara tillgängligt globalt via Fortune 500/500 då den säljs och implementeras av HCL Technologies och IBM på redan befintliga IBM-kunder.

PurpleTokenID – ”global Swish” för alla i världen

Till skillnad från system för företagsidentiteter kan PurpleTokenID också appliceras på privatpersoner för att spåra banktransaktioner, stödja alla logistikkedjor och följa alla industriprocesser, samt både skapa och skydda digitala tillgångar. Detta sker med full transparens och spårbarhet samt automatiserad clearing och settlement.

–PurpleTokenID i form av identifiering och e-wallet används bland annat för att skapa en global version av Swish till jordens fattigaste som kanske inte ens har tillgång till normala bankkonton. Vi vill med vår teknik, tillsammans med IBM och HCL, sätta ett fotavtryck på den globala marknaden för humanitär och socialt rättvis teknik för alla, samtidigt som vi bygger framtidens säkerhets- och identifieringssystem för alla banker med deras redan tagna investeringar i bagaget, säger Mikael Bramstedt.

BlueBarricade – världens snabbaste blockchain

Den kapacitet och teknologi som krävs för att skapa ett modernt IT-system för identifiering, spårning och avstämning som lever upp till lagar och regelverk finns nu tillgänglig i form av BlueBarricades blockchainprodukt 1400TPS.
Analysföretaget Gartner har uppskattat det totala marknadsvärdet för blockchain till 3,1 triljoner dollar vid utgången av år 2030.

– Inom företagsvärlden finns direkt affärskritiska processer som kräver hög transaktionshastighet och central lagring i speciella säkerhetszoner. När vi använder oss av central stordatorkapacitet på 1400 blockchaintransaktioner per sekund, eller 120 miljoner transaktioner per dygn, ändras premisserna och gör blockchain tillgänglig för exempelvis bank och finans eller tillverkande industri, säger Mikael Bramstedt.

> Den kapacitet och teknologi som krävs för att skapa ett modernt IT-system för identifiering, spårning och avstämning som lever upp till lagar och regelverk finns nu tillgänglig i form av BlueBarricades blockchainprodukt 1400TPS.

Fakta om BlueBarricade

BlueBarricade Blockchain & AI Technology AB är ett Fintech-bolag med säte i Stockholm, bildat 2018 av Mikael Bramstedt och Lars Bäck. Bolaget har i dagsläget mer än 160 aktieägare över hela världen. I en pågående nyemission har BlueBarricade emitterat 487 000 nya aktier till 20,50 EUR per aktie. Företaget har avtal med HCL Technologies och IBM om lansering och försäljning av 1400TPS på alla marknader till HCL:s och IBM:s befintliga kunder.

Läs mer på:
bluebarricade.com

Denna artikel är **i samarbete med BlueBarricade.**

PurpleTokenID

Blockchain & AI
BlueBarricade

NO MURPHY.

JUST MURPHY.

RULE CRISIS COMPLEXITY. WITH SIMPLICITY. JUST ADD MURPHY.

Att stå förberedd inför krisen handlar inte om att ta sig an dess komplexa natur och osäkra utgång med ännu mer avancerade processer och verktyg. Tvärtom. Hemligheten bakom fungerande krishantering stavas enkelhet och förberedelse. Det handlar om kontinuerlig utbildning för många, träna ofta istället för att öva sällan och intuitivt systemstöd som driver processen när krisen inträffar.

Vi kallar det Murphy's Way. För precis som Edward Murphy (Murphy's Law) älskar vi förberedelser och vet att förr eller senare drabbas de flesta verksamheter av en större påfrestning. Det är då förberedelserna är avgörande. Vi satte ihop extremt erfarna krisledare med knivskarpa utvecklare. Resultatet är Murphy Crisis Management and Training Platform. Vill du veta hur ni kan stå bättre rustade med Murphy vid en kris? Följ länken för att se filmen där Senior Advisor Mats Bohman förklarar Murphy's Way.

murphysolution.com/get-to-know-murphys-way

MURPHY SOLUTION

Stark förändring, stora möjligheter

FOTO: SÄKERHETS- OCH FÖRSVARSFÖRETAGEN

Robert Limmergård
Generalsekreterare
Säkerhets- och försvarsföretagen

Vi lever i dag i en tid med många och snabba förändringar. Inte alla är positiva. Risker och hot uppfattas hopa sig runt oss, osäkerheter eskalerar och konvergerar, geografin krymper och så även tidsperspektiven. Denna fas i utveckling – lokalt och globalt – verkar inte vara övergående, snarare tvärtom. Förändringar ger nya problem men också nya möjligheter - om vi vill och om vi agerar.

Text Robert Limmergård

Det är egentligen välkänt: i tider av kaos och höga nivåer av komplexitet förordas alltid handlingskraft, eftersom det ökar möjligheten att påverka utvecklingen. Förändringsförmåga har alltid varit ett konkurrensmedel. Att vara passiv lönar sig inte. Vi lever därför i den djärves tid.

Möta morgondagens behov

Teknikutvecklingen utgör idag, precis som tidigare i världshistorien, den säkerhetspolitiska fronten; de som aktivt söker samarbete med dem som driver utvecklingen är de som också äger framtiden. De som är passiva halkar efter. Att arbeta med, och intressera sig för, förändring är därför i högsta grad en säkerhetspolitisk fråga. Frågan om nya lösningar i totalförsvaret, däremot, är märkligt nog inte så allmänt diskuterad i det utvecklingsarbete som pågår. Detta trots att alla är eniga om att ”det gamla totalförsvaret” inte är önskvärd för att skydda morgondagens samhälle.

Samtidigt borde nya lösningar utgöra en kärnfråga när vi hanterar skyddet av vårt samhälle. Tillgången till kunskap och teknik är en förutsättning i utvecklingen av ett samhälle som är hållbart, resilient och funktionellt. Det handlar inte om att något varit dåligt tidigare, utan om att se möjligheter och möta morgondagens behov.

Företag är en del av säkerhetspolitiken

Det komplexa nuläget, teknikutvecklingen och säkerhetspolitiken är sammanvävda och företag och teknik blir alltmer i centrum för säkerhetspolitiken. Här har Sverige stora möjligheter. Sverige hamnade återigen på topplacering i FN:s Globala Innovationsindex för 2021. Det är ett skäl till att näringslivet måste spela en roll i totalförsvaret. Självklart har företag kunskap, kompetens, förmåga och resurser på som måste användas för att skydda samhället. Pandemin visade även att företag spelar en naturlig roll i försörjningsrelaterade frågor, som t.ex. produktion, lager och logistik.

> **Förändringsförmåga har alltid varit ett konkurrensmedel. Att vara passiv lönar sig inte. Vi lever därför i den djärves tid.**

Men. Det räcker inte med teknik. För att stärka samhällssäkerheten krävs att vi skapar samspel mellan lösningar, resurser och behov. Där vi låter möjligheter genomsyra utvecklingen. Där vi nyttjar de resurser vi har till förfogande – oavsett om de förvaltas av staten eller företag.

NORDIC **LEVEL** GROUP

Our **VISION**

To be the best-in-class full-service provider of critical safety and security solutions in the Nordics.

Our **MISSION**

Enabling our clients to live a levelled life.

www.nordiclevelgroup.com

Färist Mobile. På Polisens sida

Samhällsviktiga myndigheter arbetar i hårda miljöer med känslig information. Tutus har därför utvecklat en säker mobiltelefon, Färist Mobile som både tål tuffa tag och står emot kvalificerade cyberangrepp.

Ett eget operativsystem med stark diskkryptering och externa nycklar skyddar känslig information mot läckage, stöld och exponering mot 3:e land. Färist Mobile är granskad och godkänd av svenska och europeiska myndigheter för att skydda sekretessbelagda uppgifter. Genom en VPN tunnel isoleras kommunikationen från påverkan och fungerar även som en yttre gräns. Det innebär att all trafik är skyddad vare sig det är röstsamtal, meddelanden, e-post eller data.

Förutom inbyggd högupplöst kamera och skärm finns ytterligare funktioner som Push To Talk och fordonsmontage med extern touchskärm vilket gör Färist Mobile till ett säkert arbetsverktyg för samhällsviktig verksamhet!

Tutus är marknadsledare av godkända och certifierade krypto- och IT-säkerhetsprodukter i Sverige och vi gör stadiga framsteg mot målet att bli en ledande leverantör inom EU. Som ett oberoende företag samarbetar vi med näringsliv och myndigheter för att erbjuda pålitliga, säkra och kostnadseffektiva säkerhetslösningar som kan möta dagens säkerhetsbehov.

För information kontakta Mikael Andersson på mikael@tutus.se eller läs mer på **www.tutus.se**

TUTUS