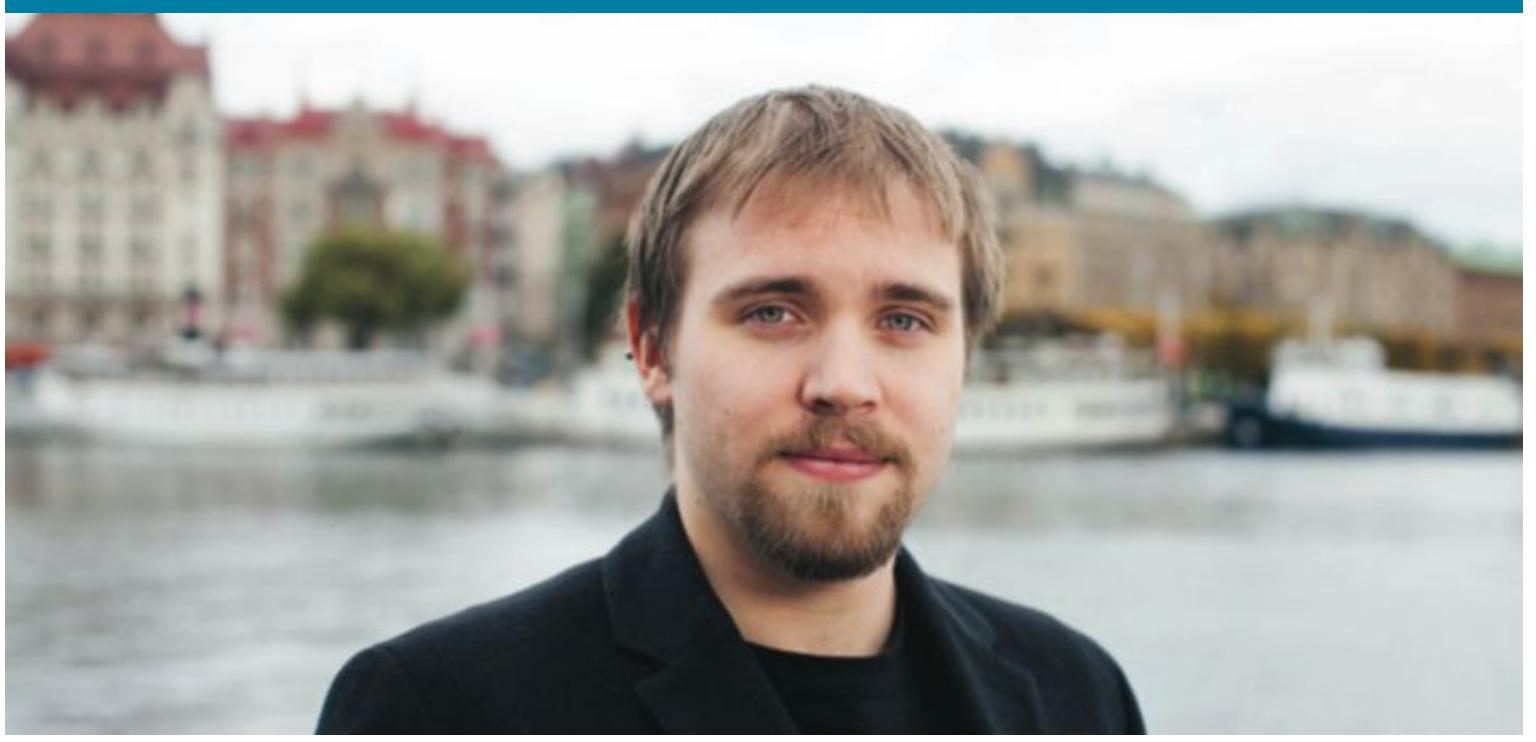
DÅLIG SÄKERHET.



» Charlie Svensson, konsult på säkerhetsföretaget Sentor vill uppmuntra företag att själva ställa krav på säkerhet då man anlitar en webbyrå.

Webbyråers slarv bjuder in hackare till företagssajter

Många företagssajter innehåller allvarliga sårbarheter. Det varnar säkerhetsföretaget Sentor som pekar ut slarviga webbyråer och dålig kravställning från kunderna som orsaken.

KARIN LINDSTRÖM
karin.lindstrom@idg.se

Företag och organisationer missar ofta att hålla koll på säkerheten på sina sajter. Tidigare var inte det något allvarligt problem – en attack mot sajten sänkte den, men det var sällan någon kom åt någon information. Så ser det inte ut längre. I takt med att kunderna förväntar sig tjänster och interaktivitet när de går in på en företagssajt så blir den även en port in för hackare.

Men det här är något som många företag inte förstår vidden av. De litar på de webbyråer de anlitar men de brister alltför ofta när det gäller säkerhetstänkande. Det anser Charlie Svensson som är konsult på säkerhetsföretaget Sentor.

– Jag skulle säga att över hälften av de sajter vi testar är öppna för exempelvis cross-site scripting.

Han berättar om företag som aldrig testat säkerheten under de tre år de haft sin sajt uppe.

– Så kommer vi och testar och inser att det gått att hacka den från dag ett. Vi vet att internet ständigt skannas av och då är det inte frågan om det läckt ut grejer från databasen – frågan är i det läget hur mycket som är ute och var det finns.

Parallellt med att hemsidorna utvecklats och blivit mer sammankopplade med de interna systemen än tidigare så har också trycket på utvecklare ökat. Det gör att de som arbetar på webbyråerna inte alltid har koll på hur man bygger för att klara säkerheten.

– Kanske man låter en praktikant hjälpa till – men att kunna programmera är inte samma sak som att förstå hur man undviker sårbarheter, säger Charlie Svensson.

RECEPTET FÖR ATT SLIPPA obehagliga överraskningar är inte så komplicerat egentligen – det handlar om att följa de ramverk som finns när man bygger sajterna.

– Kunderna måste också bli mycket bättre beställare. I dag finns inte ens säkerhet med i avtalet när man anlitar en webbyrå, eller så står det en svepande formulering om att ”säkerheten ska vara god”.

HUR GOD SÄKERHET ska tolkas har Charlie Svensson hört jurister från kunden och jurister från webbyrån diskutera under de rätt stela möten som blir resultatet av en utläckt databas.

– I stället bör kunden kräva att sajten säkerhetstestas, både under arbetet och efteråt, säger han.

– Det är ett kontinuerligt arbete.

Vilka företag är det då som drabbas? Sällan de allra största – där finns rutiner på plats.

– De minsta har vi sällan som kunder, så det vet jag inte riktigt. Bland medelsmå till medelstora företag är nog denna sortens problematik absolut vanligast – men den förekommer överallt, hela vägen upp till giganterna, säger Charlie Svensson.

FAKTA

Vanliga säkerhetsbrister

- **SQL injection-brister** som läcker ut databasinnehåll till angripare eller låter dem kapa servern, vilket öppnar för djupare intrång.
- **Cross-site scripting** är ständigt aktuellt. Används för att länka in skadlig kod som virus och trojaner. Kan även utnyttjas för att fjärrstyra besökarnas webbläsare.
- **Brister i patchningsrutiner** och **webbramverksplugins** av **tvekSam kvalitet**. Ibland ändrar man plugins så att de blir inkompatibla med originalpluginet, varefter man inte kan säkerhetsuppdatera sina plugins automatiskt längre.
- Att **driftsätta mjukvarukomponenter** som inte säkerhetstestats.
- Egna **osäkra kryptolösningar**, som innebär att angripare kan komma åt känslig information eller ta sig förbi inloggningar och liknande.
- Man **tillåter okontrollerade filuppladdningar**, vilket resulterar i att angripare kan köra godtycklig kod på servern
- Bygger **egna implementationer av komplicerade protokoll** som soap, saml eller oauth, vilket nästan alltid resulterar i att viktiga detaljer förbises och lösningen blir osäker.

Stockholmsbarn ska börja koda i skolan

Nu vill Stockholms stad slå ett slag för att få in programmering i skolan. Redan i höst drar ett pilotprojekt i gång där elever på utvalda skolor får kodning på schemat.

Kod är en del av vardagen och därför behöver fler behärska den och få bekanta sig med programmering redan i skolan. Det slår Stockholms finansborgarråd Karin Wanngård, Martin Lorentzon, grundare och ordförande på Spotify och Maria Rankka, vd på Stockholms Handelskammare fast i en debattartikel i Dagens Nyheter.

De tre pekar på att Stockholm är en innovativ stad men att det krävs en ständig utveckling för att behålla den positionen. De pekar också på att Stockholm 2011 hade den största andelen teknikjobb av samtliga större regioner i Europa, 18 procent, och att programmerare i dag är det vanligaste yrket i Stockholms län – 36 000. Trots det är bristen på utbildade programmerare ett hot mot Stockholms position och därför måste det tas krafttag för att skapa intresse redan i tidig ålder, före högskola och yrkesutbildning.

Därför är det dags att Stockholms skolbarn får ett nytt språk på schemat – kod. För att hitta vägar som på ett effektivt sätt inkorporerar det nya språket i skolorna kommer Stockholm nu att tillsätta en kommission som ska utreda hur programmering ska ta större plats i undervisningen i stadens skolor. Kommissionen ska också se hur stort utrymme som Stockholm har att ta egna initiativ eller om det finns hinder i form av statliga regler.

Redan i höst drar staden dock igång ett pilotprojekt där utvalda skolor får programmering på schemat.

» Ett pilotprojekt drar igång i höst med tidiga programspråkstudier på utvalda Stockholmsskolor.

KARIN LINDSTRÖM
karin.lindstrom@idg.se

Beslutsstöd anpassas till alla

I takt med att efterfrågan av beslutsstöd ökar i alla delar av verksamheten behöver gränssnitten anpassas efter användarna. Utmaningen för både leverantörer och kunder är att skräddarsy efter roll, kunskap och behov – utan att skapa datakaos.

Användarnas ökade krav på anpassat beslutsstöd, i kombination med it-avdelningens oförmåga att tillfredsställa detta behov, har lett till ett uppsving för lättåtkomliga självbetjäningslösningar, ofta molnbaserade. Inköpen görs ofta ute i verksamheten, vid sidan av it-avdelningen, säger Dan Sommer, svensk analytiker på Gartner.

– Användandet ute i verksamheten kan vara mångdubbelt högre än vad it-avdelningen tror, säger han.

GARTNER SPÅR att över 50 procent av alla företagsanvändare inom två år har tillgång till verktyg för ”självservering” för att på egen hand förbereda data för analyser.

Sas Institute utvecklar gränssnitt för allt fler användarkategorier. Det gäller exempelvis affärsanalytiker, controllers och marknadschefer som inte har samma kunskaper i statistik som experterna. Konceptet Guided Analytics innebär att användarnas gränssnitt skräddarsys. Att upptäcka bedrägerier, värdera risker och hantera säkerhetshot är exempel på användningsområden som kräver komplexa analyser, men allt oftare görs av användare som inte är renodlade programmerare eller statistiker.

MEN DET FINNS RISKER med för mycket anpassning. Resultatet av ren självbetjäning utan central kontroll kan bli att datakvalitet och styrning blir lidande.

– Det är en svår balansgång att inte strypa nyfikenhet och experimenterande, men samtidigt hålla kontroll, säger Dan Sommer.

Här ser beslutsstödsleverantörerna en chans genom att erbjuda både central kontroll och flexibilitet vid självbetjäningen.

– Personer ute i verksamheten kan behöva snabb och rollanpassad information för att förstå sitt bidrag till affärsmålen. Utifrån samma information kan en centralt belägen chef göra djupare analyser som ställer krav på avancerade funktioner och förkunskaper, säger Robin Askelöf, marknadschef på Hypergene.

MARTIN WALLSTRÖM
martin.wallstrom@idg.se

FAKTA

Ökat intresse kräver ökad kontroll

Gartner spår att intresset för självbetjäning kommer fortsätta öka på samma sätt som Excel gjorde för några decennier sedan. Med trenden kommer också krav på ökad kontroll i inköpen av beslutsstödet, där hela beslutsstödet är integrerat och samordnat inom företaget.