Medie världen Premium

Analys / Sakari Pitkänen

Metoder mot digitala attacker

IT-säkerhet kostar pengar. Bristande IT-säkerhet kan kosta ännu mer i takt med att digitala attacker blir allt vanligare. Men det finns strategier för hur medieföretagen ska minimera riskerna att deras sajt tas över av illasinnade hackare.

›› Det första tecknet på att TV5Monde var hackat kom den 8 april på den franska tv-jättens Twitter och Facebook-konton som plötsligt visade "Je suis ISIS". Vid tiotiden på kvällen stängdes samtliga TV5:s samtliga elva tv-kanaler ned. Det blev svart i rutan i de 200 länder dit TV5Monde sänder. Säkerhetsexperter världen över kallar attacken en av de värsta någonsin. Hackarna hade skaffat sig tillträde till social mediekonton, webbservrar och, den helt nyligen uppdaterade, Ericssonbyggda tv-plattformen.

Under tre timmar var det svart i rutan och först 18 timmar senare hade TV-5Monde full kontroll över sina system.

Den franska regeringen kallade omedelbart in företrädarna för de stora medieföretagen till krismöte för att diskutera datasäkerhetsfrågor. Händelsen inträffade bara några månader efter terrordåden mot Charlie Hebdo och vid Hyper Cache. Frankrike befann sig fortfarande i ett slags krigstillstånd med tusentals poliser och millitärer som patrullerade landets gator. Och just då tar några som säger sig vara IS över statens egen tv-kanal.

SAKARI PITKÄNEN

MEDIEKONSULT

Egen företagare och mediekonsult. Tidigare chefredaktör för Metro Sverige och Metro International. Även digital utvecklingschef och vice vd för Metros internationella webbverksamhet. Jobbade som pr-konsult 2009 till 2012.

Medie världen Premium

Det är inte känt om det verkligen var IS som låg bakom intrånget. Det finns ännu ingen officiell förklaring till hur attacken skedde.

– Det var tur för dem att angriparna valde att flagga upp att de var inne i systemen. Det hade varit värre om de legat lågt och bara samlat in all slags information, konstaterar Martin Zetterlund, grundare av säkerhetsföretaget Sentor som bland annat arbetat med flera medieföretag i Sverige.

Somligt tyder på att såväl stater som organisationer som IS och Al Qaida har ökat aktiviteten mot medieföretag. Men det är svårt att veta exakt. Det kan lika gärna vara "vanliga" hackare som använder sig av den för tillfället mest omtalade organisationen för att de vet att det skapar uppmärksamhet. Oavsett om det är terrorgrupper eller tonåringar får internationella konflikter återverkningar på svenska och internationella mediers IT-säkerhet. Några exempel:

✷ Dagen innan TV5-incidenten varnade FBI i USA för att "individer som sympatiserar med Islamiska Staten IS" utnyttjar säkerhets hål i WordPress-plattformen som används av många medieföretag i större eller mindre utsträckning.

✷ Expressen har en mindre del av sin produktion på WordPress, bland annat underavdelningen Mitt Kök. Avdelningen blev hackad av någon som utgav sig för att vara IS. Samtidigt blev flera andra siter som artisten Shirley Clamps hemsida, Västerås flygplats webb med flera utsatta för liknande attacken.

✷ I mars drabbades ETC.se av någon som bland annat beskrev sig som Hacker of Islam.

✷ I maj fick franska Le Soir stänga ned sin sajt på grund av intrång. Samtidigt hackades flera andra franska och beligiska medier. De senaste rapporterna tyder på att två tonåringar stod bakom. En av dem angavs för övrigt av hackargruppen Anonymous, eftersom den är för pressfrihet...

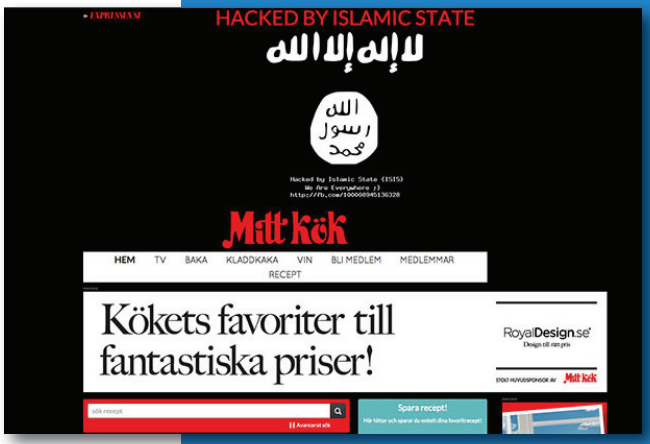
✷ I maj togs togs Washington Posts webb över för en kort tid av Syrian Electronic Army, en grupp som sägs stödja Assad-regimen i Syrien.

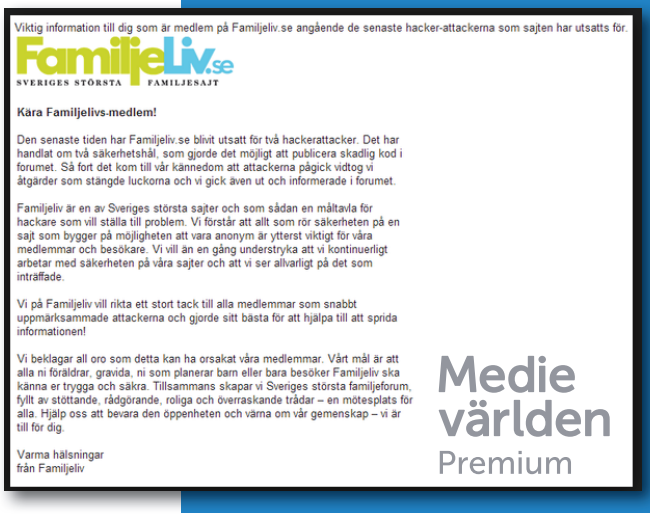
Dessutom har Familjeliv.se och flera västsvenska tidningar, bland andra Alingsås Tidning blivit hackade under våren. Många incidenter är "automatiska". En mjukvara scannar nätet för att hitta siter som har säkerhetsluckor som kan utnyttjas på olika vis. I de fallen är inte offren medvetet valda, de råkar bara hamna på scanningens lista.

Många utomstående analyser av TV5-attacken pekar mot att det som i säkerhetsvärlden kallas social engineering, är en trolig förklaring. Med det avses att hackarna tar sig in i företags digitala system via en personlig kontakt med någon på insidan av brandväggar och andra

250 miljarder spam – per dag

Spam – skräppost – är fortfarande ett vanligt sätt för ovälkomna besökare att ta sig in på olika nätverk. Talen är så stora att det är svårt att tro på dem. Men enligt välrenommerade Ciscos Senderbase skickas det över 250 miljarder skräpmeddelanden om dagen. Bara 13 procent av all e-post som skickas är legitim. Resten är spam. Sverige ligger i den övre fjärdedelen av spamdränkta länder.





säkerhetssystem. Det kan vara en länk i ett pressmeddelande, mail eller en annons. Möjligheterna att komma in i ett mediehus är oändliga: medierna är ju till sin natur öppna och lever av att kommunicera.

– Vi har haft den typen av försök. Men de har avslöjats av våra anställda innan något hänt, säger **Peter Frey,** IT-chef på Expressen och tidigare Aftonbladet. Han är övertygad om att behovet av investeringar i IT-säkerhet kommer att öka för medieföretag, och har oroat sig för just en attack av det slag som skedde på TV5Monde. Att angriparen tar sig in innanför brandväggen och kan börja penetrera olika delar av företagets nätverk: annonsservrar, webbservrar eller – i värsta fall – CMS:et som gör det möjligt att publicera eller ändra det som redan är publicerat.

– Jag tror att vi kommer att gå ännu mer mot att ha olika säkerhetsnivåer på olika data. "Det här (till exempel CMS:et) är heligt". Där ställs de hårdaste kraven medan andra delar kan vara mindre säkra, men samtidigt inte gå att använda som väg in till de säkra delarna.

Medieföretag har alltid varit utsatta för risker. Den stora skillnaden är att riskerna tidigare var lokala. Dagens hackare, virusspridare, överbelastnings-attackerare och IT-utpressare är globala.

En attack kan komma varifrån som helst. Det kan vara IS eller en supermakt lika gärna som en tonåring på Västgötaslätten. Hittills har den senare kategorin troligtvis utgjort det största hotet mot svenska medieföretag. Många företag ser en tydlig uppgång i försök till överbelastningsattacker, "DDoS", under skolloven. Det kostar bara några tiotals dollar att köpa sig ett bot-net som kan överbelasta dåligt konfigurerade servrar. I de flesta fall handlar det om ren skadegörelse. Värre är de som tar sig in i systemen för att stjäla information. Men det kan även handla om att bevaka medieföretag av politiska skäl. 2013 avslöjade New York Times att deras system blvit utsatt för en sofistikerat

"JAG TROR ATT VI KOMMER ATT GÅ ÄNNU MER MOT ATT HA OLIKA SÄKERHETS-NIVÅER PÅ OLIKA DATA. 'DET HÄR (TILL EXEMPEL CMS:ET) ÄR HELIGT'. DÄR STÄLLS DE HÅRDASTE KRAVEN MEDAN ANDRA DELAR KAN VARA MINDRE SÄKRA"

Medie världen Premium

intrångsförsök. Enligt tidningen kunde attacken spåras till Kina. Händelsen sammanföll dessutom med att New York Times höll på med ett undersökande reportage om korruption högt upp i den kinesiska politiska hierarkin.

I några fall kan det även vara en form av utpressning, "Om ni inte betalar fortsätter vi att sänka er sajt". Den sortens affärsverksamhet har fått ett eget namn: Ransom ware.

Utpressning har under de senaste åren blivit enklare tack vare – eller på grund av – bitcoins. Den virtuella valutan kräver varken fysisk överlämning eller går att spåra i efterhand. Det finns ett antal fall bland svenska lokaltidningar där angriparen tagit sig in på webbservern och krypte-rat en stort antal filer. Därefter har ledningen fått meddelande om att filerna kan öppnas igen, om tidningen betalar motsvarande 300 dollar i bitcoins. Det är oklart om tidningen betalade eller inte.

Överhuvudtaget är det svårt att med bestämdhet veta något om säkerhetsfrågor. Branschen, det vill säga de som livnär sig på att sälja system för att undersöka, övervaka och stoppa attacker, har ett kommersiellt intresse av att ringa i larmklockorna. Å andra sidan har många brottsoffer goda skäl till att inte berätta om att de utsats för IT-brott.

Brottsstatistiken talar dock sitt tydliga språk. Under de senaste åtta åren har datorbedrägerier sexdubblats i Sverige, sådana som klassas som med "internet som hjälp" har ökat från 1 500 fall 2006 till drygt 23 000 förra året. Den absoluta merparten av anmälningar kommer från privatpersoner.

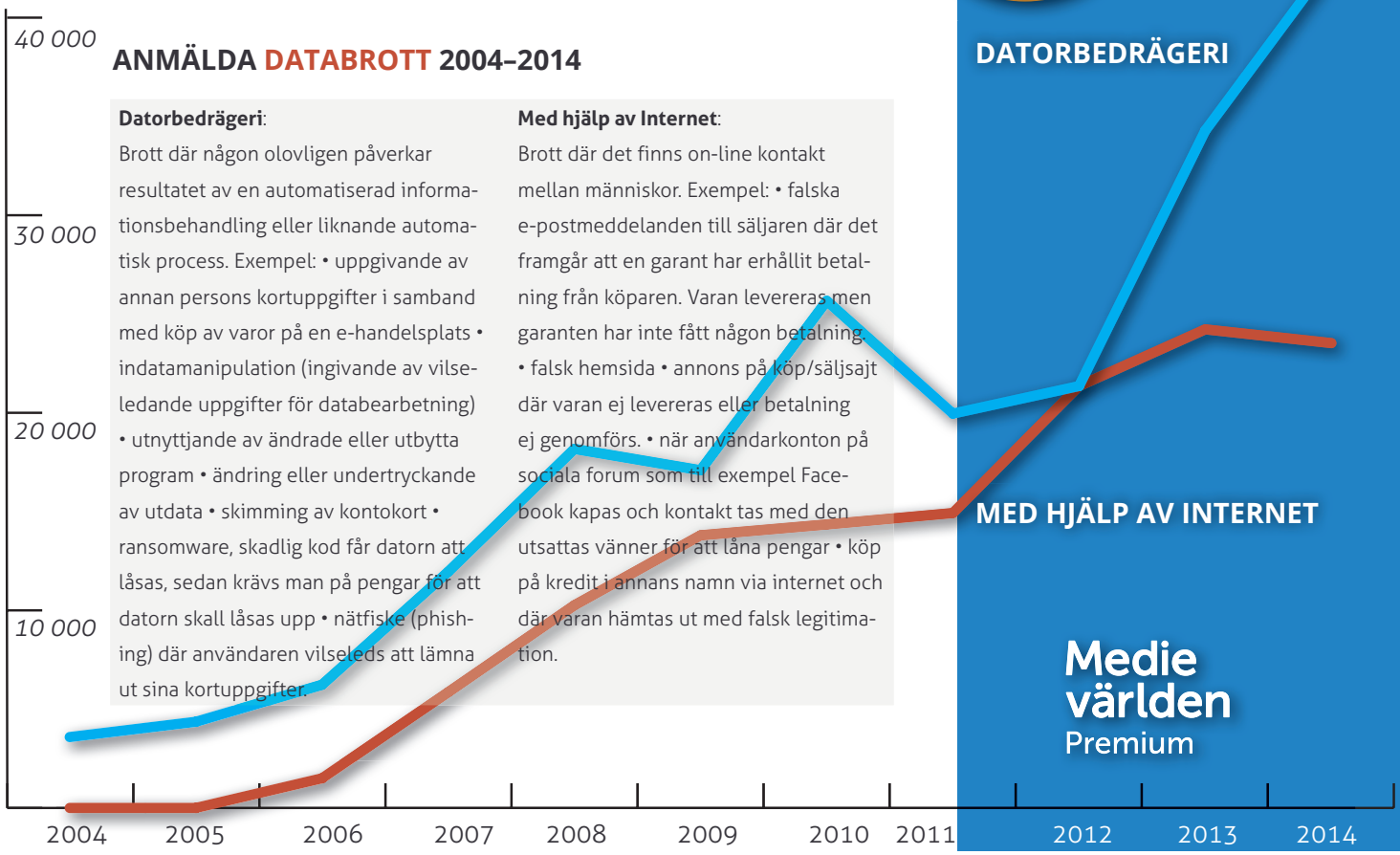
Förbannade hackare slog till mot Aftonbladet

Vintern 2008 avslöjades att den beryktade gruppen "Vuxna Förbannade Hackare" tagit sig in Aftonbladets IT-miljö. Omfattningen av intrånget är fortfarande oklart, men de hade tillgång till lösenord för mailkonton för anställda. Händelsen är ingående beskriven i Daniel Goldberg och Linus Larssons bok "Svenska hackare".

- Hacket mot Aftonbladet var riktigt allvarligt och omfattande, säger Linus Larsson som i dag bevakar IT för Dagens Nyheter.

Hur ska medier förhålla sig till att skriva om attacker som drabbar det egna företag?

- Jag tror inte någon seriös redaktion skulle skriva under på att allvarliga dataintrång ska mörkas av strategiska skäl. Däremot händer det att rätt triviala hack blir uppblåsta. Det riskerar att utmåla grupperna bakom dem som mäktigare än de är. Inte minst gäller det överbelastningsattacker, som är rätt enkla att genomföra, säger Linus Larsson.



Datorbedrägeri:
Brott där någon olovligen påverkar resultatet av en automatiserad informationsbehandling eller liknande automatisk process. Exempel: • uppgivande av annan persons kortuppgifter i samband med köp av varor på en e-handelsplats • indatamanipulation (ingivande av vilseledande uppgifter för databearbetning) • utnyttjande av ändrade eller utbytta program • ändring eller undertryckande av utdata • skimming av kontokort • ransomware, skadlig kod får datorn att låsas, sedan krävs man på pengar för att datorn skall låsas upp • nätfiske (phishing) där användaren vilseleds att lämna ut sina kortuppgifter.

Med hjälp av Internet:
Brott där det finns on-line kontakt mellan människor. Exempel: • falska e-postmeddelanden till säljaren där det framgår att en garant har erhållit betalning från köparen. Varan levereras men garanten har inte fått någon betalning. • falsk hemsida • annons på köp/säljsajt där varan ej levereras eller betalning ej genomförs. • när användarkonton på sociala forum som till exempel Facebook kapas och kontakt tas med den utsattas vänner för att låna pengar • köp på kredit i annans namn via internet och där varan hämtas ut med falsk legitimation.

Medie världen Premium

Det är logiskt att riskerna ökar ju mer digitiserade och internetanslutna företagen blir. Medieföretag är särskilt utsatta eftersom de är kända. Ju större desto kändare, desto större risk. Mediernas affärsidé bygger på öppenhet och kommunikation med användarna. I dag mycket mer än förr då nästan alla medarbetare förväntas föra dialog på sociala medier för att sprida sin journalistik.

Hoten är många och säkerhet kostar. Center for Strategic and International Studies har uppskattat den totala kostnaden för cyberbrott i världen till 0,8 procent av världen BNP, väsentligt mer än till exempel världens samlade bistånd. Undersökningen är visserligen finansierad av ett säkerhetsföretag men siffrorna är hisnande, mellan 375 och 575 miljarder dollar beräknas nätbrott av skilda slag kosta samhället. Källa: http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2-summary.pdf

Hur skyddar man sig som medieföretag?

– Det viktigaste är att företagen tillsätter en person som är ansvarig för IT-säkerheten och som får ett tydligt mandat, säger Martin Zetterlund.

Viktigaste att tänka på

Enligt Expressens IT-chef Peter Frey:

- Anlita ett säkerhetsföretag för en oberoende undersökning.
- Gå igenom realistiska scenarion kring säkerhet för att se hur det ligger till "Datahall brinner upp", "Nätverket hackat", "Sajterna nere på grund DDOS, "All användardata på vift", "Alla företagets lösenord publicerade på Flashback" etc.
- Prioritera säkerhetsluckorna och riskerna.
- Arbeta långsiktigt med säkerhetsfrågor – inte bara när det krisar.
- Avsätt ordentligt med tid, pengar och resurser.
- Överlåt inte säkerhet bara till it-avdelningen utan gör det till en angelägenhet för hela företaget.

Hackare inte det enda hotet

Efter Snowdenavslöjandena vet vi att medier underrättelse- och säkerhetstjänster granskar i stort sett all verksamhet på nätet. Svenska FRA däremot säger sig ha vidtagit åtgärder för att inte övervaka svenska medier – en handling som skulle vara olaglig. Men Internetstiftelsen påpekar i sin årsrapport om säkerhetsläget på nätet att: "Även om FRA själva påstår att de har infört tekniska filter som ska skydda journalister på medieredaktioner i Sverige från att bli avlyssnade av FRA så tror vi att det är bättre att själv ta kontrollen över det skydd man behöver."

Det säger lagen

Den som olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling eller olovligen ändrar, utplånar, blockerar eller i register för in en sådan uppgift döms för dataintrång till böter eller fängelse i högst två år. Detsamma gäller den som olovligen genom någon annan liknande åtgärd allvarligt stör eller hindrar användningen av en sådan uppgift.

Är brottet grovt, döms för grovt dataintrång till fängelse i lägst sex månader och högst sex år. Vid bedömande av om brottet är grovt ska det särskilt beaktas om gärningen har orsakat allvarlig skada eller avsett ett stort antal uppgifter eller annars varit av särskilt farlig art. Lag (2014:302).

Lästips:

Myndigheten för Säkerhet och Beredskap MSB har publicerat en guide för hur man kan förbereda sig för överbelastningsatttacker som fortfarande utgör en stor och irriterande del av hackerkulturen. Guiden är skriven för kommuner men lämpar sig lika bra för medier.

www.msb.se/RibData/Filer/pdf/27385.pdf

Medie världen Premium