DATAFÖRENINGEN

Dataintrång hos Dataföreningen

Annica Bergman Dataföreningen i Sverige
Internetdagarna 21 oktober 2008

Dataföreningen i Sverige

- Dataföreningens verksamhet omfattar drygt 26 000 medlemmar, fördelade på sex kretsar med aktiviteter i 105 nätverk. Under 2007 arrangerades drygt 500 aktiviteter som samlade totalt ca 7000 deltagare

Vad jag kommer att prata om!

- Dag 1
- Dag 2
- Dag 3-4
- Dag 5-10
- Dag 11-90

RING MIG OMEDELBART

DATAFÖRENINGEN

Vi har blivit hackade!

Samtal till kontoret 28 feb strax efter 16
från Blekinge tekniska högskola
IT-chefen i Östersund, vd i Oslo, ordförande
i Åre och nyckelperson i Indien
(utan omvärldskontakt)

Vad ?

Uppgifter om alla medlemmars

- användaridentitet
- lösenordet krypterat (hashat)
- e-postadress

hade publicerats på Flashback.se tillsammans med publiceringen fanns information från hackarna, som kallar sig Vuxna Förbannade Hackare.

Kort om teknisk miljö och drift

DATAFÖRENINGEN I SVERIGE

www.dfs.se microsoftmiljö egenutvecklad applikation

Den Fjärde Dimensionen

www.d4d.se Linux och Drupal MySQL

IT-drift och förvaltning outsourcad

WM-data a tagicaSVEA company

QBRANCH:

Kreawit

Dag 1

- 17:15 hade jag verifierad information om det inträffade och båda sajterna var avstängda
- 18:30 hade krishanteringsgruppen (styrelsen) första telefonmötet
- även informationsansvarig var informerar och uppmanad att förbereda ett pressmeddelande
- 19:45 går pressmeddelande ut
- 20:45 skickas epost till alla medlemmar
- Polisanmälan gjordes
- Teknisk arbete med servrarna påbörjas och pågår hela natten

Omvärlden

Stort angrepp mot Dataföreningen - mängder av lösenord i spridning

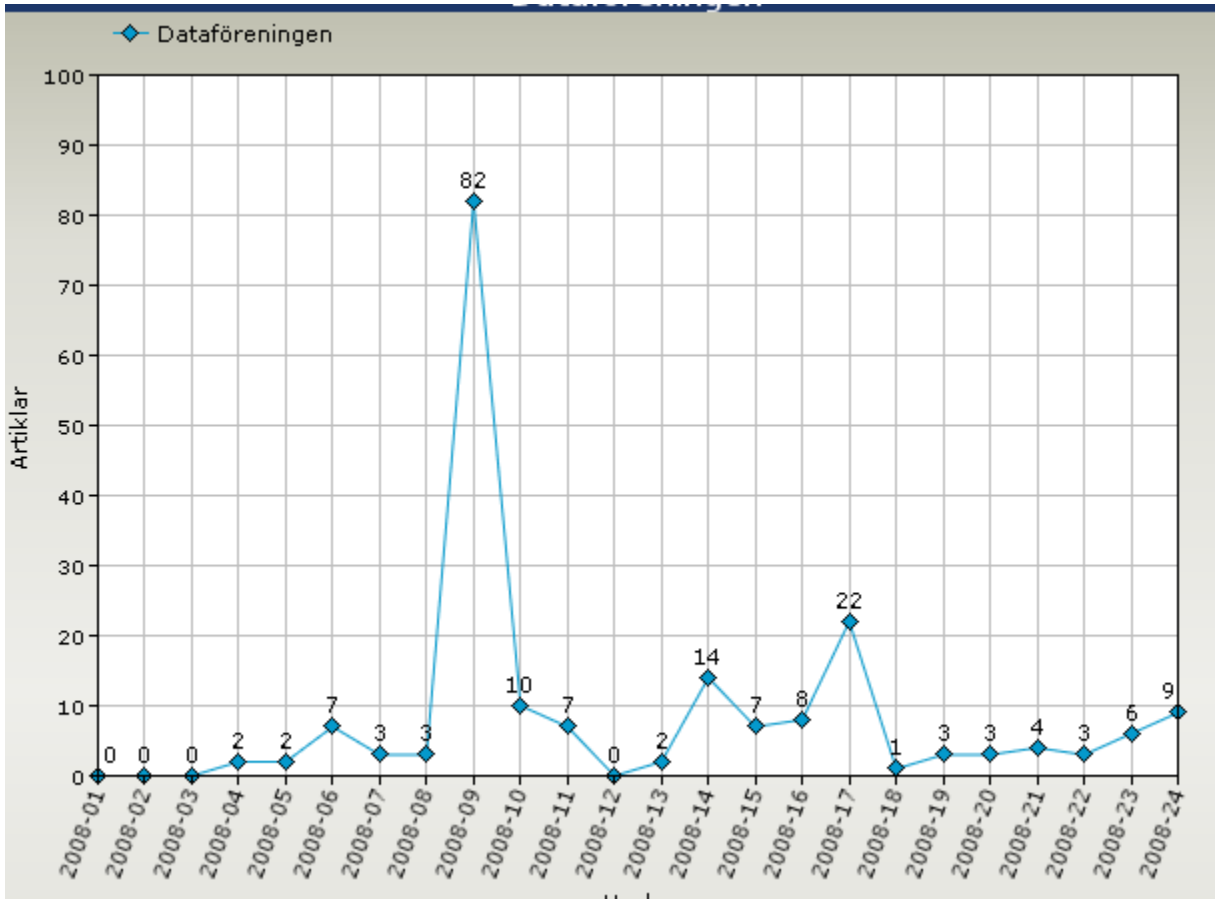
Av Joel Brandell | Tech

Efter en tid av lugn har "Vuxna förbannade hackare" återigen gått ut med lösenordsuppgifter som man kommit över genom ett hack. Den här gången är det medlemmar i Dataföreningen som drabbats.

- Massmedia ringer oavbrutet, dag 1 sista samtalet efter klockan 24 fortsätter dag 2-4
- Rykten
- Kommentarer till artiklar i forum

Hackare börjar dekryptera lösenorden och listor med dessa publiceras bl.a. på pastebin.com

Media!



Mycket press – hur vända det negativa till något positivt?

Varför hacka Dataföreningen?

Dataföreningen sitter på lösningen för att förhindra nästa hackarvåg

- fre, 2008-01-25 10:46

Ämnen: Oppna Standarder IT-säkerhet OpenID

Vi använder allt fler e-tjänster idag, informella och formella. Lösenord och koder fungerar bäst när vi kan memorera dem och de är unika i varje sammanhang. Vi har sett konsekvenserna av attackerna mot Aftonbladet och Bilddagboken.se i närtid, hur polisers e-postkonton med känsliga uppgifter kommit på awägar, vi har sett hur databaser med uppgifter om tusentals kommunala och statliga tjänstemän kommer på awägar. Det grundläggande problemet är att det inte längre är möjligt att använda lösenord och koder som det ursprungligen är tänkt. Vi kan helt enkelt inte hålla allt i huvudet längre utan börjar återanvända samma lösenord på flera ställen. Att använda samma lösenord på flera ställen är i sig inte ett problem, problemet ligger på ett administrativt plan och ett sårbarhetsplan. Lösenordets hemlighet blir aldrig högre än dess svagaste förvaringsplats. Lösenordet nedskrivet på en lapp under tangentbordet eller lagrat i klartext i en slarvigt hållen databas spelar mindre roll, det kommer på awägar och ger otillbörlig tillgång till en mängd tjänster. Lösenordet kan heller inte administreras enkelt, för att behålla styrkan i bra lösenord så måste de förnyas regelbundet. Det är

Röster från medlemmar

- Jättebra hanterat från er sida! Om det är något tröst i det hela…Jag tror ni har gjort alla rätt kommunikationsmässigt.
- KLANTSKALLAR ! Det här är ju inte kul alls
- Mycket pinsammare än så här blir det inte. Sme'ns häst var de facto sämst skodd.
- Mycket bra initiativ att så här snabbt skicka ut ett brev om det inträffade.

Jag besvarade själv cirka 200 telefonsamtal de 2 första dagarna. Totalt fick vi runt 1000 mail där vanligaste frågan var vilket lösenord man hade - vilket vi inte kunde besvara. Endast en bråkdel av all mail var negativ i övrigt var den saklig eller av karaktären ”synd att det här har hänt men kämpa på”

Dag 2

- Internt möte på kansliet direkt på morgonen
- Genomgång av olika informationsflöden och målgrupper
- Fortsatt proaktiv information men också många samtal och mail att besvara. (krisledningsgruppen, kanslier m.m.)
- Snapshot av nuvarande servrar slutfördes
- Sammanlagt fem resurser fortsätter nattens arbete med att lokalisera säkerhetshål allt pekar på d4d.se
- Ny virtuell server är uppsatt för den drabbade miljön
- Ytterligare resurser kallas in för att generera nya lösenord

Dag 3 och 4 (helg)

- Fortsatt arbete med sajterna för att lokalisera var intrånget har skett
- Fortsatt arbete med att säkra sajterna
- Tekniska åtgärder verifieras av extern säkerhetsexpert.
- Beslut att skicka ut nya lösenord med vanlig post kontakter med leverantör för distribution samt dialog kring lösenordets styrka, beslut att gå PTS rekommendation

Vi öppnar igen på måndag!

- Säkerhetsgenomgång på applikationsnivå på dfs.se visar bland annat på risker för SQL-injection
- SQL-injection är ett sätt att utnyttja säkerhetsproblem i hanteringen av indata i vissa datorprogram som arbetar mot en databas.
- Attacken uttnyttjar inte någon ny svaghet i IIS eller SQL-server utan helt enkelt det faktum att dynamisk SQL tillåts köra med parametrar som hämtas direkt från formulär eller Querystrings. **Därför är det också i huvudsak äldre webbapplikationer som kör 'klassisk' ASP som drabbats**.
- Den äldre webbapplikation som vi är på väg att stänga ner visar sig ha problem med SQL injection

Dag 5 till 10

- Sajterna öppnar - inledningsvis med begränsad funktionalitet
- Problemen med sql-injection på dfs.se blir tydligare och mer omfattande
- Följde upp polisanmälan
- Skrev till engelska DI och flashback

Dag 11- 90

- Omfattande dialog med verksamheten om funktionalitet
- Prioriteringsdiskussioner och kontinuerliga beslut
- Utveckling av tillfälliga lösningar (som kan permanentas om så beslutas)
- Trötta men inte utmattade

Slutnota över 1 miljon kronor

- Stänga befintlig miljö och säkerställa bevarande
- Sätta upp och verifera ny miljö
- Säkerhetsrevisioner i flera omgångar
- Porto och administrativa kostnader
- Utveckling av tillfälligt verksamhetsstöd
- + egna resurser totalt cirka 0,5 personår (inkl IT, medlemservice m.m.)

Lärdomar!

- Jag borde ha initierat en säkerhetsrevision på IT-systemen första dagen på jobbet!
- Var extremt försiktig vid flytt av miljö, koll på filer m.m.
- Ha bra loggning
- Givetvis patcha systemen och bra rutiner för test och driftsättning
- Använd inte skarp data i testmiljön
- Driftsleverantörer är inte bättre på det här än andra, skriv bra SLA och använd tredje part för att verifiera säkerheten

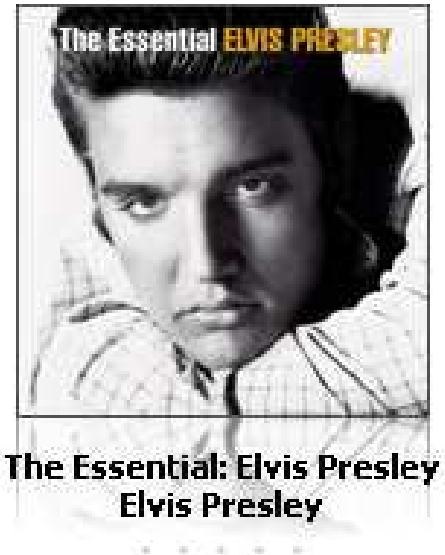
Lärdomar!

- Vissa informationstexter kan skrivas i förhand
- Bättre ordning på distributionslistor
- Säkerställ resurstillgång via SLA innan det händer
- Bevaka Flashback.se
- Censurera medlemmarnas bloggar ;-)

annica.bergman@dfs.se
08-587 434 00

DATAFÖRENINGEN

Lite hjälp att hålla humöret uppe!



”Are You Lonesome Tonight”

Kontaktuppgifter
annica.bergman@dfs.se
0706 096665