Whitepaper

KASPERSKY lab

TIO SÄTT
för cyberbrottslingar att utnyttja IT-avdelningars svagheter

Be Ready for What's Next.

Tio sätt för cyberbrottslingar att utnyttja IT-avdelningars svagheter

Om du inte redan har gjort det så ska du först läsa Kaspersky Labs tekniska dokument ”Det pågår ett krig”. Du kan hämta och läsa dokumentet i resursavsnittet. ”Det pågår ett krig” behandlar cyberbrottslingarnas verkliga mål, de anställda eller rättare sagt deras utrustning. Dokumentet fokuserar på hur IT-avdelningar omedvetet gör cyberbrott möjliga genom att ge cyberbrottslingar tillgång till system och data tack vare en rad med missuppfattningar och felaktiga antaganden.

Slutanvändarens behov av åtkomst till Internet och kommunikationskanaler dit har exploderat. Även företagen får allt större behov av fler kommunikationskanaler. Kombinationen av de anställdas mobilitet och affärsdata medför ökade utmaningar, och att hålla de exponentiellt växande hoten från cyberbrottsligheten stången känns snart sagt ogörligt. Många IT-avdelningar har blivit ”medbrottslingar” till cyberbrottslingarna utan att veta om det eller ens förstå det. I det här dokumentet behandlas de olika svagheter som kan finnas hos ett företags IT-avdelning och som cyberbrottslingarna utnyttjar. Även riktlinjer för hur denna farliga, destruktiva utveckling kan förhindras diskuteras.

Dokumentet beskriver de 10 sätt som cyberbrottslingar kan utnyttja dagens IT-avdelningar på samt metoder för att stoppa dem, baserat på forskning från tredjepart och analyser från Kaspersky Labs experter. Hur klarar sig ditt företag från dessa alltför vanliga fallgropar?

Svaghet nr 1
Anta att data finns i ett datacenter

Beakta det faktum att de flesta chefer har en kopia av e-posten i sin smartphone (iPhone, BlackBerry osv.), en andra kopia på sin bärbara dator och en tredje kopia i företagets e-postserver. Det visar tydligt att det finns dubbelt så mycket data utanför datacentret som i det. Lägg sedan till otaliga USB-minnen, CD-skivor, säkerhetskopior, molnbaserade lösningar och datautväxling med affärspartners så växer snart antalet platser långt utöver vad vi normalt förväntar oss.

Intuitivt förstår vi att data knappast är under kontroll, men ändå behandlar IT-avdelningen hot med utgångspunkt i att data är under kontroll. Varför skulle annars så oproportionerligt mycket tid och pengar spenderas på att förstärka datacentrets gränssnitt med tekniker som t.ex. autentisering, åtkomsthantering, brandväggar och program mot nätverksintrång osv. Därmed inte sagt att dessa tekniker inte behövs. Det gör de definitivt. Men vi måste koncentrera oss på de platser där data är just nu, dvs. hos användarna.

Data finns inte i ett skyddat lager. Data rör sig fritt utanför datacentret. Faktum är att IDC:s undersökning visar att stationära och bärbara datorer utgör den största oroskällan för att förlora data. Det är hos slutanvändarna som det finns ett direkt hot mot dataförluster. IDC:s undersökning visar även att mobila enheter är den främsta anledningen till nya säkerhetsinvesteringar. Fler företag vidtar åtgärder för att förbättra säkerheten även utanför datacentret.

Tio sätt för cyberbrottslingar att utnyttja IT-avdelningars svagheter

Svaghet nr 2
Inte inse värdet av mobila enheter

Tid är pengar. Otaliga timmar ägnas åt att producera rapporter och analysera data för att kunna göra väl underbyggda affärsbeslut. E-post besvaras och presentationer sammanställs under helger och all data sparas i våra bärbara enheter. Affärsmöjligheter utvärderas löpande så att det går att reagera snabbt när chanser ges ändå behandlar IT-avdelningarna bärbar utrustning som om den vore innehållslös. När en utrustning blir stulen gäller försäkringsanspråket endast värdet av den försvunna utrustningen och de värdefulla data som fanns i den ignoreras. Det leder till att skyddet för mobila enheter vanligtvis koncentreras på värdet av enheten istället för värdet av data i den. Faktum är att i de flesta fall är data i enheten värda hundratals gånger mer än själva enheten.

Att använda administrerade antivirusprogram, stöldskydd och integritetsskydd för mobila enheter är en bra början för att skydda mobila data. Företagen låter ofta användarna välja tillverkare och modell helt valfritt när de köper affärskritiska mobila enheter som t.ex. bärbara datorer och smartphones. Det växande antalet iPhones i företagsnätverken är ett bra exempel. Tyvärr är de flesta affärsmän och IT-avdelningar mer bekymrade över tiden och kostnaderna för att ersätta själva enheten än de värdefulla data som fanns på enheten.

Anställda utrustas med enheter efter eget val istället för de enheter som är bäst på att hantera antivirusprogram och stöld- och integritetsskydd. Som en följd härav innehåller företagets nätverk en kompott av enheter, operativsystem, operatörer, säkerhetsprofiler och olika teknologier. För en organisation med begränsad säkerhetsbemanning kan kravet på att garantera säkerheten, oavsett plattform, vara mer än de klarar av.

Svaghet nr 3
Villfarelsen att företagets bärbara datorer och mobila enheter aldrig används för privat bruk och att affärsdata därför inte läcker till privata system

Vi kan inte längre anta att företagets utrustning endast används i jobbet. Bärbara datorer fungerar t.ex. som kommunikationskanal och transaktionsverktyg för affärsmän på resande fot. Sociala nätverk används för att hålla kontakt och program som t.ex. Skype används för att hålla kostnaden för utlandssamtal låg. Inköp av IT-utrustning sker mer och mer på konsumenternas villkor och de anställda förväntar sig flexibilitet och valfrihet även när det gäller enheter som företaget administrerar.

Många anställda använder sina privata datorer för att komma åt affärsdata efter kontorstid. Om enheterna inte är ordentligt skyddade utgör de en ökad risk för säkerhetsluckor. Användningspolicy och ett administrerat säkerhetsprogram är nödvändigt för att säkerställa ett ordentligt dataskydd där även personalens privata utrustning kan ingå. Många företag utökar sina investeringar och licenser för säkerhetsprogram till att gälla även de anställda för att utvidga skyddet av viktiga data. All information som lagras inom företagets nätverksgränssnitt på mobila enheter som t.ex. en smartphone, bärbar dator eller minidator borde krypteras med tanke på hur lätt det är att en sådan enhet glöms, förloras eller stjäls.

Svaghet nr 4
Mobila enheter jämställs med stationära datorer

För några år sedan var företagens IT-nätverk väl definierade inom fasta gränser. I skyddsteknologierna kunde en tydlig gräns dras mellan vad som var internt och externt för nätverket. Gränsen kunde liknas vid en medeltida vallgrav där externa enheter ansågs vara osäkra medan de interna skyddades av företagets brandvägg likt slottet innanför vallgraven. Företag runt om i världen ser nu stora fördelar med att utrusta medarbetare som arbetar på distans eller mobilt. Utvecklingen inom mobilteknologi låter företagen skapa ”den ständigt uppkopplade medarbetaren” som har full tillgång till affärskritiska företagsresurser, t.ex. program, dokument och e-post, från var som helst i världen under sina resor. Handhållna enheter ingår i medarbetarnas utrustning och anställda på resande fot kan ansluta till företagets nätverk och data från flygplatser, hotellrum och flygplan, trots att ingen av dessa Internet-anslutningar är säker. Arbetsdagen är inte längre begränsad till kontorstid. Personalen uppdaterar information, svarar på kundkontakter och hanterar alla de vardagliga göromålen - dygnet runt. Denna miljö har dock skapat nya sårbarheter hos företagen och de kommer säkerligen att utsättas för ökande hot (Mobile Security - IDC).

Tio sätt för cyberbrottslingar att utnyttja IT-avdelningars svagheter

En stark säkerhetspolicy för bärbara datorer måste vara diametralt olik policyn för stationära datorer. För stationära datorer som endast används på arbetsplatsen behövs inga specialtekniker som t.ex. separata brandväggar., en bärbar dator behöver skyddas i varje specifik arbetssituation. När den lämnar den relativa säkerheten i företagets nätverk ska säkerhetsprogrammet vara programmerat så att säkerheten automatiskt höjs. Säkerhetsåtgärder, som t.ex. att aktivera en brandvägg, stänga av en icke lösenordsskyddad Bluetooth-anslutning eller trådlös anslutning och öka granskningen av USB-enheter, ska aktiveras automatiskt när en bärbar dator lämnar företagets nätverk.

Svaghet nr 5
Användning av sociala medier utan skydd

Sociala medier har kommit för att stanna. Denna nya ”oumbärliga” teknologi utgör ett tillväxtsegment i verksamheten. Den kan ha stora positiva effekter, rätt hanterad.

För tio år sedan var IT-avdelningarna starkt fokuserade på att få grundläggande åtkomst till Internet och sedan kom behovet av företags-e-post och därefter chattprogram. Alla är idag verksamhetskritiska verktyg och sociala medier är bara nästa i raden som vi måste förbereda oss inför. Många företag brottas med frågan hur de ska låta sina anställda använda Web 2.0-verktyg på ett ansvarsfullt sätt utan att offra säkerhet eller införa stränga föreskrifter för användning. Sociala medier och Web 2.0-teknologier kan, om de används på ett säkert sätt, gagna samarbete och produktivitet såväl som företagens vinster. Företagen bör fokusera på hur sociala medier ska kunna införlivas på ett säkert sätt eftersom det med några få undantag skulle bli opraktiskt att helt bannlysa sociala medier.

Det är viktigt med en formell policy för åtkomst till och administration av sociala medier. Om ett företag t.ex. skyddar sitt nätverksgränssnitt mot attacker från sabotageprogram, men saknar nödvändig kontroll över anslutningar till sociala nätverk, kan en oförsiktighet av en anställd leda till att företagets nätverk infekteras. Det kan förorsaka betydande ekonomiska förluster, antingen direkt eller indirekt. Det är även möjligt att anställda frivilligt läcker information till tredjepart via sociala medier.

Med undantag för några få mycket kontrollerade akademiska miljöer är det opraktiskt att bannlysa sociala medier. Ett mer praktiskt tillvägagångssätt är att utnyttja tekniker som noggrant övervakar trafiken till och från de sociala mediernas webbplatser och blockerar osäkra webbplatser.

Svaghet nr 6
Fokus på skydd istället för detektering och respons

När en heltäckande säkerhetsplan övervägs är det flera funktioner som måste beaktas. De grundläggande funktionerna är skydd, detektering och respons. Antivirusprodukter är ofta förbisedda och betraktas som ett produktinköp som görs automatiskt varje år. Det betyder att möjligheterna till detektering och respons också förbises. Som vi har visat är dessa element avgörande i en säkerhetsstrategi. Det finns dessutom ett stort spektrum av skydd, prestanda, administration, spridningskapacitet och support i branschen.

Tio sätt för cyberbrottslingar att utnyttja IT-avdelningars svagheter

Många företag skiftar fokus mot nya säkerhetstekniker som DLP, kryptering osv. Det här är värdefulla verktyg och ändå fortsätter det totala antalet incidenter och infektioner med skadlig programvara att växa. En undersökning av IDC visar att 46 % av företagen upplever en ökning av incidenter med sabotageprogram och endast 16 % en minskning. Skillnaden i uppfattning är ännu större bland små och medelstora företag (500 - 2 499 anställda) där 44 % ser en ökning och 7 % en minskning. Det innebär att sabotageprogram fortfarande slipper igenom de förstärkta skyddsåtgärderna och det betyder i sin tur att ett ännu större fokus måste läggas på funktioner för detektering och respons. IT-avdelningar investerar i skyddsåtgärder vid gatewayen, samtidigt som personalen tillåts surfa på Internet. Cyberbrottslingarna bjuds in med vidöppna dörrar när tillräckliga resurser för detektering och blockering saknas.

Eftersom dagens cyberbrottslingar riktar in sig på användarnivån måste kraftfulla detekterings- och responstekniker användas i användarnas utrustning. Utrustningen måste skyddas från cyberbrottslingarnas sabotageprogram som är konstruerade för att stjäla data, inloggningsuppgifter och pengar.

Svaghet nr 7
Dålig information om betydelsen av vaksamhet

Användarens vaksamhet och kunskap är avgörande för informationssäkerhet på alla nivåer. De anställda måste t.ex. informeras om hur de ska skydda sig mot sabotageprogram, hur de surfar säkert, hur de undviker spyware och scareware, hur bilagor ska hanteras. Företagets lösenordspolicy måste vara känd för alla anställda och lösenord måste användas. Även företagets Internet-policy måste vara känd, övervakas och användas.

Kännedom om hot, deras påverkan och spridningsmetoder hjälper till att hålla användarna vaksamma och hindrar dem från att fatta dåliga beslut som skulle kunna infektera deras utrustning. Kampanjer om säkerhetsmedvetenhet på en regelbunden basis är avgörande för att hålla de anställda informerade och skyddade. Det är naturligtvis lika viktigt att även IT-personalen är välinformerad om aktuella hottekniker och attackvektorer så att välunderbyggda beslut kan fattas om skydd och skyddstekniker.

Svaghet nr 8
Ovilja att rapportera säkerhetsbrister

Även om cyberbrottsligheten har ökat med över 23 %, och kostnaden för säkerhetsbrister mer än fördubblats är det bara toppen på ett isberg. Data som presenteras av FBI är dessutom en underskattning eftersom företagen inte alltid rapporterar om att de har utsatts för ett brott. Företagen vill helt enkelt inte att någon ska få veta att de har blivit utsatta för brott av rädsla för att värdet på deras aktier eller deras varumärke och goodwill ska påverkas negativt.

Även om det är en naturlig impuls att dölja attackerna blir resultatet en skev bild av den växande hotbilden över Internet. Rapporteringsoviljan ger ett falskt intryck av att hotet från skadliga program är minimalt och ökningen av cyberbrott överskattad. Sanningen är att ökningen är betydligt större än 23 %. FBI kan helt enkelt inte kvantifiera ökningen närmare eftersom så många oanmälda brott begås varje dag.

Ditt företag har stor nytta av att känna till att det förekommer brott, hur de utförs och hur företaget kan skyddas mot liknande attacker.

Svaghet nr 9
Följa föreskrifter

IT-säkerhet är inte alltid detsamma som att följa föreskrifter. Det är lätt att uppfylla säkerhetsföreskrifter utan att säkerhet uppnås. Många företag betraktar skydd mot sabotageprogram som en engångsinsats: ”Jag får väl skaffa det och underhålla det, men det får räcka”.

Föreskrifter utformas ofta som toppstyrning. En filtermall för cookies är ett vanligt exempel. Företaget måste ta hänsyn till sina egna produkter och räkna ut hur de fungerar med mallen. Säkerhet som byggs upp på rätt sätt byggs upp underifrån. Oavsett om du konstruerar ett program eller arkitekturen för företagets nya nätverk måste säkerhetsaspekten beaktas. När du t.ex. konstruerar arkitekturen för en produkt är det lika viktigt att bygga in säkerhetselementen i programmets arbetskopior som att kommunikation, lokalisering, versioner osv. ska fungera redan från början. Säkerhetselementen ska sedan följas upp och förbättras under utvecklingen. Föreskrifter kan ge en illusion av säkerhet för den som inte förstår hur komplex dagens digitala affärsvärld är. Föreskrifter får aldrig vara slutmålet.

Svaghet nr 10
Anta att allt är OK

Även om system kan verka fullständigt säkra är det trots allt människor som hanterar dem. I många fall är det den mänskliga faktorn som förorsakar problem på grund av misstag, okunskap eller bristande rutiner. Företagets personal behöver utbildning om informationshantering, hur de bör agera i olika situationer, hur de ska följa företagets säkerhetspolicy och säkerhetsrutiner, hur de undviker sabotageprogram genom att vara vaksamma och försiktiga och, i det fall de redan är infekterade med skadliga program, hur de skyddar sina data och förhindrar framtida förluster.

Gör en ordentlig kontroll av risken för säkerhetsincidenter i din egen verksamhet. Allt är inte OK.
Vi kan alla göra ett bättre jobb för att försäkra oss om att verksamhetskritiska data inte kommer i obehöriga händer.

Sammanfattning

Varje dag hittar cyberbrottslingarna på vägar att infiltrera utrustningen hos företagets användare, enbart med syfte att stjäla data och pengar. Enligt rapporten ”The Top Cyber Security Risks” från SANS.org förlorar företag tusentals dollar varje dag trots att de tror att de är säkra.

Vi kan alla göra ett bättre jobb för att säkra vår verksamhet kritiska data får inte komma i obehöriga händer

Kaspersky Lab AB
Färögatan 33
164 51 Kista
Sweden

+46 8 5785 3000
corporatesales@kaspersky.se

www.kaspersky.se
www.securelist.com
www.threatpost.com

3x4a