PHYSICAL MEETS DIGITAL

BÄSTA PRAXIS INOM CYBERSÄKERHET

IRON MOUNTAIN®

BÄSTA PRAXIS INOM CYBERSÄKERHET

Dataintrång är ett växande problem för världens organisationer, vilket framgår tydligt av siffrorna:

- **Nära hälften** av respondenterna i en studie bland 4 200 företag i Europa och USA uppger att de har råkat ut för ett dataintrång under det senaste året[1].
- Den **genomsnittliga kostnaden** för ett dataintrång uppskattas till 3.86 miljoner dollar.

Affärsrisken kopplad till ett dataintrång eller en läcka är inte bara storleken på eventuella viten. Ryktesspridning, fallande aktiekurser och förlust av kundernas förtroende är minst lika allvarliga risker att väga in då de har potential att skada ett varumärkes anseende i grunden.

Det finns många verktyg för företag som vill försöka skydda sig mot intrång och avvärja attacker. I den här artikeln lyfter vi blicken mot informations- och cybersäkerhetsfrågorna i ett vidare perspektiv. Hur kan du **implementera bästa praxis** för cybersäkerhet i hela verksamheten för att garantera datas **konfidentialitet, integritet** och **tillgänglighet** – och samtidigt säkra upp återställningen av dina data i händelse av ett intrång?

1. Hiscox/Risk based security: 2017 Data Breach QuickView Report

MÅSTE ALLA FÖRETAG (OAVSETT STORLEK) BRY SIG OM CYBERSÄKERHET?

Hackare och databrottslingar struntar i storleken. Även om storföretagens enorma volymer kunddata kan vara frestande, finns tillräckligt mycket att tjäna på att komma åt ett mindre företags leverans- och betalningslösningar.

På sitt sätt är problemet större för små och medelstora företag. De har ofta snäva säkerhetsbudgetar, samtidigt som minsta nedtid kan få förödande konsekvenser för ekonomin.

FÖRSTÅ HOTBILDEN

Vet du vilka hot som finns och hur de kan påverka ditt företag? Det finns många att förhålla sig till.

- Statistiken visar att skadlig kod, eller **malware** – malicious software, fortsätter att vara det största hotet som kräver daglig hantering. Datavirus, ormar, trojaner och spionmjukvara (sk. spyware) är olika typer av skadlig kod. Ett enkelt klick på en till synes oskyldig länk kan vara allt som krävs för att släppa in elakartad mjukvara som skadar företagets IT-miljö.

- **Ransomware**, eller gisslanmjukvara, blir allt vanligare. Ett företag kontaktas av en cyberbrottsling som säger sig ha infekterat dess IT-system med skadlig kod och kräver en lösensumma för att häva infektionen. Företaget kan inte veta säkert om hotet är sant eller om det löser problemet att betala ut beloppet. Helt säkert är dock att det skulle få allvarliga konsekvenser om den skadliga koden tilläts infektera systemen.

- **Phishing-attacker**, **nätfiske**, riktar in sig på användare. Med hjälp av mer eller mindre trovärdiga e-postmeddelanden försöker bedragare förmå människor att lämna ifrån sig personuppgifter, ekonomiska data eller säkerhetskoder för att lura av dem pengar.

FÖRSTÅ DE DATA DU HAR

Det finns även många andra typer av attacker från ett brett spektrum av spelare, från enskilda stater som bedriver spionage till organiserad brottslighet och "hacktivister". Med en växande marknad för så gott som alla typer av data lär cyberattackerna fortsätta utvecklas i snabb takt vad gäller form, skala och förfining. Experterna är överens - frågan är inte om du kommer råka ut för ett intrångsförsök, utan när det kommer att ske. Så det gäller att vara redo. Att utveckla en strategi för att förhindra dataintrång och attacker är nödvändigt för företag av alla storlekar.

Vet du vilka data ni har i era system, och varför ni har dem? Utsätter ni data som företaget egentligen inte ens borde ha tillgång till för onödig risk?

ATT FÖRSTÅ DATA ÄR ETT VIKTIGT FÖRSTA STEG

Att hantera och skydda data effektivt och i enlighet med lagen är avgörande. Det krävs god datastyrning (data governance) parat med en djup förståelse för organisationens data- och informationsflöden, för att kunna säkra data i livscykelns alla steg.

SKAPA EN RISKBASERAD STRATEGI

De tre primära riskerna är **affärsmässig verksamhetsrisk, risk kopplad till anseende** och **legal risk**, det vill säga risk kopplad till **efterlevnad av lagar**. Även om det inte finns någon patentlösning för cybersäkerhetsarbete, är det värdefullt att sluta upp kring något av de etablerade standardramverk som finns, exempelvis ISO 27001 inom EU (eller NIST, US National Institute of Standards i USA).

Hör med ditt försäkringsbolag vilket ramverk som är bäst lämpat för just ditt företags behov.

BEAKTA HELA AFFÄRSPERSPEKTIVET

Cybersäkerhet handlar inte bara om teknik. Det är en korsfunktionell disciplin där IT, juridik och säkerhetsexpertis behöver samverka för att utmana hot. Och det är en fråga för varje enskild medarbetare som måste vara medveten om hur lätt det är för obehöriga att ta sig in.

FOSTRA EN SÄKERHETSMEDVETEN FÖRETAGSKULTUR

Den mänskliga faktorn är avgörande för att skapa en säker miljö.

Sårbarheter uppstår sällan av medveten illivilja, men ett oskyldigt klick på fel knapp kan vara tillräckligt för att släppa in fel spelare i systemet.

Medarbetare måste känna till potentiella risker och förstå vilka skyldigheter de har. Ett medvetet, långsiktigt arbete med att medvetandegöra säkerhetsfrågorna är nyckeln till framgång. Företaget bör erbjuda kontinuerlig utbildning, anpassad för respektive mottagare, som förklarar vikten av ett säkert arbetssätt och konsekvent efterlevnad av policier.

Samtidigt gäller det att hålla ett öga på missnöjda anställda, eller tidigare anställda, genom att:

- **Övervaka beteenden** för att uppmärksamma uppenbara tecken på missnöje.
- **Implementera processer** för att kunna flytta på medarbetare som medför en risk.
- Införa rollbaserad **åtkomstkontroll**, som begränsar tillgången till kritiska datasystem.

LÄS MER ▷

UTVECKLA EN STARK STYRNING

För att din cybersäkerhetsstrategi ska bli framgångsrik i verksamheten krävs **styrning och ledarskap**. Affärsverksamheten måste **anpassas till säkerhetsstrategin**, för att mildra effekten av dataintrång och optimera fördelningen av säkerhetsresurser.

Stark säkerhetsstyrning kräver följande:

- Uttalat stöd från högsta ledningen.
- En dedikerad person med uttalat mandat att ansvara för cybersäkerhet.
- Tydliga policier, processer och procedurer.
- En stark cybersäkerhetskultur.
- En åtgärdsplan för incidenthantering.

BYGG FÖRSVARET PÅ DJUPET

Kontrollsystem och skalskydd kan fallera. Se till att ha en strategi för att skydda företagets datatillgångar på djupet, hela vägen från perimeterskyddet till ändpunkten. Om en angripare tar sig in innanför den yttre försvarslinjen, finns kompletterande skydd på plats längre in i strukturen.

Fysisk säkerhet bör sätta stopp för obehörig åtkomst. Dessutom måste traditionella säkerhetsåtgärder - som nätverks- och systemkontroller, brandväggar och intrångsdetektering - kombineras med mer avancerade verktyg för att avvärja hot.

KATASTROFÅTERHÄMTNING - PLANERA FÖR DET VÄRSTA

Många företag har planer för katastrofåterhämtning **(disaster recovery)** och **affärskontinuitet (business continuity)**. Men historiskt har de förberett sig på fysiska olyckor, som översvämningar och eldsvådor, snarare än cyberangrepp – trots att dessa kan tillföra nog så stora skador.

Tänk igenom vilken inverkan en välriktad cyberattack skulle få på din verksamhet och förbered dig på att hantera den.

Frågor att ställa till din verksamhet är:

- Hur länge kan ni överleva ett avbrott och vilka är de kritiska tillämpningarna som måste återställas så fort som möjligt? Små företag är exempelvis känsligare än stora om attacken påverkar kassaflödet.
- Hur mycket får det kosta att säkra verksamheten mot angrepp? En redundant lösning, där data lagras på flera noder, är exempelvis dyrare - men också mer effektiv.
- Har du vägt in alla aspekter av redundans i den fysiska miljön, hela vägen ned till fibern som levererar uppkoppling till och från datacentret?
- Tränar du medarbetarna i hur de ska agera i händelse av dataintrång? Testar du återställningssystemen regelbundet? Deltar externa partners och leverantörer i övningarna?

En formell åtgärdsplan gör det enklare att hantera angrepp – och återhämta sig från dem.

I praktiken innebär det att sätta ihop ett dedikerat incidenthanteringsteam som tränas löpande. Repetera planen, genomför skrivbordsövningar och simuleringar och planera för hur fel orsakade av den mänskliga faktorn kan minimeras. En god idé är att ta hjälp av ett företag som är specialicerat på incidenthantering – och målstyra det på att incidenter inte inträffar.

- Ha en plan för krishantering som adresserar både interna och externa intressenter – och säkerställ att planen planen följs för att bibehålla förtroendet.
- Ha beredskap i form av alternativa kommunikationskanaler på plats, eftersom de normala kommunikationsvägarna riskerar att sättas ur spel vid en incident.
- Slutligen, se till att ni har bra back up-rutiner.

SE VÅR VIDEO OM ATT BYGGA EN PLAN FÖR ÅTERSTÄLLNING AV DIN DATA

BYGG DIN PLAN FÖR DISASTER RECOVERY OCH BUSINESS CONTINUITY!

LÄS MER ▷

AGERA SNABBT VID INCIDENTER

Genomsnittstiden för att upptäcka en dataläcka är 197 dagar och det tar ytterligare 69 dagar att åtgärda den[2]. Ju fortare du agerar, desto mindre skada och lägre kostnad är tumregeln. Företag som täpper till en läcka på mindre än 30 dagar uppger sig ha sparat över en miljon dollar.

RAPPORTERA DATAINTRÅNG OMDELBART

Om och när ditt företag – trots alla planer – ändå utsätts för dataintrång ska du rappotera incidenten så fort som möjligt. Även om du kan behöva uppdatera rapporten i efterhand måste du agera direkt. Det kan spara företaget enorma summor om det blir aktuellt att betala böter.

HÅLL DIN PLAN AKTUELL

Data är ett rörligt mål. Nya tekniker, system och lösningar når världens verksamheter i ett aldrig sinande flöde. Håll dig uppdaterad om nyheterna och ta höjd för dem i säkerhetsarbetet.

Spjutspetsteknik som **artificiell intelligens (AI) och maskinlärande (machine learning)** kan användas för att förbättra skyddet, men cyberbrottslingarna har naturligtvis samma fördel och kan dra nytta av teknikerna vid angrepp.

Cybersäkerhet kommer fortsätta vara en katt och råtta-lek, det avgörande är att hålla sig på tårna.

VÄLJ DATACENTER MED OMSORG

Om du väljer att **outsourca dina system** till ett datacenter hos en betrodd tredjepart, har du som kund rätt att ställa frågor om precis allt – från den fysiska miljön till policier och processer. Godkänner du de aktiviteter som tillåts i miljön? Har ni ett tjänstenivåavtal, SLA, som säkerställer att ni meddelas vid dataintrång? Har ni revisionsrätt? Kan du lita på att leverantören arbetar enligt etablerade standarder för informationssäkerhetshantering, som ISO 27001?

UTVÄRDERA DINA LEVERANTÖRER OCH PARTNERS

Hur bra du än är på cybersäkerhet är din verksamhet ingen isolerad ö. En kedja är aldrig starkare än sin svagaste länk...

Håll koll på dina leverantörer och partners och försök så långt det går att granska dem på samma sätt som du skulle gjort med ditt eget företag – även om det inte alltid är så lätt.

2. IBM/Ponemon Institute: 2018 Cost of a Data Breach

TA HJÄLP UTIFRÅN OM DU INTE KAN GÖRA ALLT SJÄLV

En konsult kan gå igenom dina datatillgångar för att avgöra hur de ska placeras och klassificeras, samt tillämpa metoder för att bedöma hotbilden.

Mindre företag har sällan utrymme för att engagera en säkerhetsansvarig på heltid. Bättre är att hitta en **lämplig partner** som kan komma in ett par gånger per år för att gå igenom systemen och ge råd. Denna partner ska också kunna aktiveras akut i händelse av oegentligheter eller misstänkt intrång. Företagets försäkringsbolag kan föreslå en pålitlig partner.

Ju mer du investerar i **säkerhetsutbildning**, desto större är sannolikheten att det blir bra. Många utbildare idag erbjuder tester för att förstärka kunskaperna, utöver ordinarie övningar.

Om du inte kan engagera en tredje part finns **online-resurser** som SKA och IACPA. Du kan också ladda ned mallar för hotbedömning på nätet för eget bruk.

VILL DU HA MER INFORMATION OM KONTROLL, SKYDD OCH OPTIMERING AV AFFÄRSKRITISKA SYSTEM I DAGENS HYBRIDA INFORMATIONSLANDSKAP?

LADDA NED VÅR E-BOK NU ▷

OM IRON MOUNTAIN

Iron Mountain Incorporated (NYSE: IRM), grundat 1951, är ett världsledande företag inom lagring och infromationshantering. Företaget anlitas av över 225 000 organisationer i världen och förfogar över 93 miljoner kvadratmeter lagringsyta vid 1 450 fysiska enheter i 56 länder. Iron Mountain lagrar och skyddar miljarder värdefulla handlingar, inklusive affärskritisk information, extremt känsliga data samt kulturella och historiska objekt. Företaget tillhandahåller lösningar för säker lagring och arkivering av information, informationshantering, digital transformation, säker destruktion samt data center, molntjänster, logistik och förvaring av konst. Iron Mountain hjälper sina kunder med att minimera risker, efterlevnad av regler och återhämtning efter katastrofer samt med att möjliggöra digitala arbetssätt. Besök www.ironmountain.se för mer information.

IRON MOUNTAIN®

VI SKYDDAR DET DU VÄRDERAR HÖGST