En ny studie från Accenture visar att 87 procent av alla cyberattacker förhindras

Trots det utsätts organisationer i snitt för 30 dataintrång per år, vilket visar på ett fortsatt behov av investeringar för att förbättra cybersäkerheten.

Stockholm, 1 juni, 2018 – I takt med att antalet ransomware- och DDoS-attacker ökar har det genomsnittliga antalet riktade cyberattacker per organisation mer än fördubblats – Under 2017 skedde 232 attacker jämfört med 106 attacker under 2016. Samtidigt blir företag allt bättre på att upptäcka och blockera dessa attacker, enligt en ny studie från Accenture.

Trots betydande framsteg inom området, investerar endast två av fem organisationer i teknologier som exempelvis maskininlärning, artificiell intelligens (AI) och automation. Det visar att det finns mer att vinna på att investera i innovativa lösningar för cybersäkerhet.

Studien, som genomfördes från januari till mitten av mars 2018, undersöker så kallade riktade attacker. Riktade attacker har förmåga att tränga igenom nätverksskydd och skada eller extrahera värdefulla tillgångar och processer inom organisationer. Trots att trycket från denna typ av attacker mer än fördubblats från föregående år, visar studien att organisationer blivit bättre på att stoppa cyberattacker. Idag lyckas företag avvärja 87 procent av alla riktade attacker, jämfört med 70 procent under 2017. Detta innebär att 13 procent av de riktade attackerna ändå lyckas ta sig förbi nätverksskyddet, och företag utsätts i genomsnitt för 30 säkerhetsintrång per år, som antingen skadar eller leder till förlust av värdefulla tillgångar.

"Endast en av åtta riktade cyberattacker lyckades, jämfört med en tredjedel förra året. Det tyder på att företagen gör ett bättre jobb med att förhindra att data blir hackad, stulen eller läckt. Även om studien visar att organisationer blivit bättre på att begränsa effekterna av cyberattacker, finns det fortfarande mycket kvar att göra. Företag som fortsätter att investera i ny teknik kan nå en hållbar cybersäkerhetsnivå inom de närmaste två till tre åren. Det borde ses som en uppmuntrande prognos för många företagsledare.”, säger Emil Gullers, ansvarig för Accenture Security i Sverige.

IT-team upptäcker dataintrång snabbare

Studien visar också att det går snabbare att upptäcka säkerhetsintrång. Från att ha tagit månader, eller till och med år att upptäcka, kan en cyberattack numera upptäckas redan inom ett par dagar. Idag uppger 89 procent av respondenterna att deras säkerhetsteam, i genomsnitt, upptäckter brott inom loppet av en månad, jämfört med endast 32 procent i fjol. För det senaste året uppger 55 procent av företagen att det i snitt tar en vecka eller mindre att upptäcka intrång, jämfört med 10 procent förra året.

Även om företag blir allt snabbare på att upptäcka intrång, upptäcker företag fortfarande inte mer än 64 procent av alla cyberattacker - ungefär samma andel som under förra året. Företag är även i hög grad beroende av samarbete med externa aktörer för att stoppa dataintrång. Över en tredjedel (38 procent) av respondenterna säger att de tagit hjälp av utomstående experter eller konkurrenter för att detektera cyberattacker i samband med att det egna IT-teamet misslyckats, vilket motsvarar en ökning på 15 procent från föregående år. Intressant nog identifieras endast 15 procent av oupptäckta intrång genom brottsbekämpning, en markant minskning från förra årets 32 procent.

Adressera cybersäkerhet inifrån och ut

I genomsnitt anger respondenterna i undersökningen att endast två tredjedelar (67 procent) av det egna företaget aktivt skyddas av företagets cybersäkerhetsprogram. Siffror visar även att hotet från internattacker är fortsatt stort, då två tredjedelar av alla attacker kommer från den egna organisationen i samband med oavsiktliga offentliggöranden av information.

När företagsledarna tillfrågades om vilka förmågor som var mest nödvändiga för att fylla luckorna i sina cybersäkerhetslösningar var de två främsta svaren analys av cyberattacker, och bevakning av potentiella hot (46 procent vardera). Studien visar också att företag förstår värdet av att investera i ny teknik, där en stor majoritet av respondenterna (83 procent) är eniga om att ny teknik som artificiell intelligens, maskin- eller djupinlärning, användarbeteendeanalys och blockchain är avgörande för att säkra organisationernas framtid.

Fem åtgärder som organisationer kan genomföra för att stå emot cyberhot:

1. **Bygga en stark grund**: Identifiera värdefulla tillgångar och stärk deras skydd. Se till att säkerhetskontroller implementeras genom hela företages värdekedja, inte bara inom företagets egna funktioner.
2. **Simulera ett dataintrång:** Öva på att hantera dataintrång genom att simulera attacker. Låt en del av företagets IT-team planera och genomföra ett dataintrång som resterande ska detektera och förhindra. Detta gör det möjligt för IT-teamet att analysera sitt tillvägagångssätt och se vad som behöver förbättras.
3. **Nyttja banbrytande teknik**: Frigör kapital för investeringar i teknik som kan automatisera ditt dataskydd. Använd automatiserade verktyg för planering och samordning av cybersäkerhet, samt vid analys av beteendemönster i samband med intrång.
4. **Var proaktiv och använd: ”threat hunting”**: Utveckla skräddarsydd strategisk och taktisk dataskyddsintelligens för att identifiera potentiella risker. Kartlägg avvikande aktivitet vid tidpunkter då risken för en attack är extra hög.
5. **Utveckla CISO:ns roll:** Utveckla nästa generations CISO – Den som har rollen som CISO bör ha god kännedom om företagets verksamhet, och förmåga att balansera företagets säkerhetinsatser utifrån verksamhetens risktolerans.

I studien, 2018 State of Cyber Resilience, tillfrågade Accenture 4 600 företagssäkerhetsexperter som företräder företag med årliga intäkter på 1 miljard dollar eller mer i 15 länder. Syftet med studien är att förstå i vilken utsträckning företagen prioriterar säkerhet, effektiviteten av nuvarande säkerhetsinsatser och om befintliga investeringar är tillräckliga. Mer än 98 procent av respondenterna var de viktigaste eller enda beslutsfattarna avseende strategier och utgifter i samband med cybersäkerhet inom respektive organisation.

För mer information om studien, ladda ner 2018 State of Cyber Resilience.

###

För mer information, vänligen kontakta:

Anna Markelius
Marknadschef, Accenture
Tel: +46 (0) 73 051 34 52
E-post: anna.markelius@accenture.com

Om Accenture

Accenture är ett ledande globalt företag med verksamhet inom strategi, konsulttjänster, digitalisering, IT och verksamhetsoptimering. Genom branschledande erfarenhet och specialistkunskap inom olika branscher och affärsfunktioner hjälper vi våra kunder att förbättra sina resultat och skapa långsiktigt hållbara värden. Vi jobbar i gränslandet mellan IT och affär, och har över 442 000 medarbetare och kunder i drygt 120 länder. Genom innovation strävar vi efter att göra världen till en bättre plats. Besök oss gärna på https://www.accenture.com/se-en/