Två sätt att hantera en kris

Post: Hamnparken 2, 573 35 Tranås
info@tucsweden.se

Tel: 0140-44 45 10

www.tucsweden.se

Kursuppgift inom	Kommunikation och affärsmannaskap
Författare	Matti Heinonen
Utbildning	Systemutvecklare.NET
Lärare	Daniel Ström
Tranås	2021-09-27

Sammanfattning

Denna rapport börjar med inledningen som beskriver vad ämnet består av, vilka företag jag valt och varför jag valt dessa. Det är företagen Garmin och Twitter.
Därefter kommer frågeställningar jag valt ut baserat på värdet av informationen som dessa kan ge, dessa frågeställningar är följande:

Vad råkade företaget ut för?
Hur märkte de att de blivit hackade?
Vad för åtgärder vidtogs?
Hur kommunicerades det ut till allmänheten?

I Metod beskrivs kortfattat hur jag funnit informationen som ligger till grund för rapportens innehåll.

I Bakgrund hänvisar jag till hemsidor och vilket innehåll jag hämtat från respektive.

I Resultat framgår svaren på frågeställningarna jag listat här ovanför. Jag har försökt hålla det objektivt och gör inget ställningstagande.

I Diskussion tar jag ställning till hur de båda företagen hade kunnat agera annorlunda och nämner olika sätt i hur man allmänt kan förbereda sig mot framtida hackerattacker ur ett företags synpunkt.

Innehållsförteckning

Inledning **1**
Syfte och frågeställning **1**
Litteraturöversikt **1**
Metod **1**
Bakgrund **1**
Resultat **3**
Diskussion **5**
Källförteckning **7**
Bilagor **7**
Figur- och tabellförteckning **7**

Inledning

Denna rapport behandlar och analyserar två olika företag som drabbats av intrång i deras interna datasystem. Rapporten beskriver vad respektive företag har drabbats av för typ av intrång, hur intrånget genomfördes, hur företaget drabbades, hur företaget hanterade intrånget och vad konsekvenserna blev av respektives åtgärder.
Rapporten går även igenom vad som kunnats göra annorlunda, fördelar och nackdelar med de olika agerandena och hur framtida intrång kan förhindras eller försvåras.
Jag har valt att jämföra Garmin och Twitter då skillnaderna i angreppet och skillnaderna på hur de löste situationen skiljer sig så markant från varandra och en jämförelse mellan dessa kan ge en nyanserad bild av händelserna.

Syfte och frågeställning

Syftet med rapporten är att visa på skillnaderna i de båda företagens agerande, försöka att objektivt förklara varför de gjorde som de gjorde och belysa för – och nackdelar med agerandet samt belysa konsekvenserna av agerandet i nutid och vad det kan ha för konsekvenser framöver.

Frågeställningar:
Vad råkade företaget ut för?
Hur märkte de att de blivit hackade?
Vad för åtgärder vidtogs?
Hur kommunicerades det ut till allmänheten?

Litteraturöversikt

Inget att tillägga, informationen fick jag via hemsidor och står under avsnittet Bakgrund med länkar och beskrivningar.

Metod

Jag har genomgående sökt online om information om båda företagen och läst på många olika hemsidor från olika källor för att få en samlad helhetsbild kring händelserna. Länkar med beskrivning ligger i avsnittet Bakgrund.

Bakgrund

Hemsidor jag använt och beskrivningar om vad jag hämtat ovanför varje länk:

dfs.ny.gov/Twitter_Report

(Gäller information om Twitterhändelsen)
Beskriver mycket utförligt händelseförloppet från början till slut och jag anser att Department of Financial Services är en pålitlig informationskälla.

terranovasecurity.com/garmin-security-breach/
(Gäller information om Garminhändelsen)
Beskriver detaljerat om hur Garmin påverkades och hur de agerade.
Dessutom finns en numrerad lista med bra tips på hur man i framtiden blir säkrare mot liknande attacker och hur man allmänt höjer IT-säkerhetsnivån i ett företag.

Information om Garmin-händelsen:
www.businessinsider.com/garmin-paid-multimillion-dollar-ransom-to-hackers-report-2020-8?r=US&IR=T

Garmins pressmeddelande:
www.garmin.com/en-US/newsroom/press-release/uncategorized/2020-garmin-issues-statement-on-recent-outage/

Information om lösensumman angående Garmin.
news.sky.com/story/garmin-obtains-decryption-key-after-ransomware-attack-12036761

Information om Coinbase, som förhindrade tusentals transaktioner av bitcoin till bedragarna på Twitter:
www.bbc.com/news/technology-53485170

Fler hemsidor med relevant information, dessa innehöll samma information jag hittade mer utförligt på andra hemsidor.

Pctidningen.se
computersweden.idg.se
techworld.idg.se
di.se

Resultat

Vad råkade företaget ut för?
Företaget Garmin blev utsatta för en så kallad RansomWare-attack, vilket innebär att någon tagit sig in i deras interna datasystem och sedan manipulerat företagets datafiler med ett skadligt program för att därefter begära en lösensumma för att företaget åter ska få kontroll över filerna. Programmet i fråga kallas för RansomWare, vilket ungefär har innebörden ”GisslanProgram”, filerna i datasystemet hålls som gisslan tills lösensumman är betald och kan låsas upp efter att gärningsmännen skickat en kod,en så kallad krypteringsnyckel till det drabbade företaget.
Själva intrånget till datasystemet sker genom att ett falskt email skickas till företagets datorer och en ovetande anställd öppnat mailet och/eller klickat på en skadlig länk, denna metod kallas nätfiske alternativt phishing.

Företaget Twitter råkade i sin tur ut för en äldre typ av bedrägeri där bedragarna ringde upp anställda på företaget och påstod sig vara från IT-supporten på företaget.
De sade sig ringa för att hjälpa de anställda att lösa problem som uppstod när de anställda arbetade hemifrån eller på annan ort och försökte logga in på företagets interna system. Detta var ett problem som fanns på Twitter på den tiden och bedragarna hade tillräckligt med information om de anställda som skulle luras för att kunna verka legitima.
De anställda skrev sedan in sina inloggningsuppgifter på en mycket snarlik men falsk hemsida och bedragarna kunde därmed stjäla uppgifterna. De loggade sedan in på Twitters äkta interna system med den anställdes uppgifter och bytte deras lösenord för att bibehålla kontrollen av kontot.
Hackarna laddade bland annat ned all information från 7 användare, twittrade bedrägliga länkar från 45 stycken och totalt användes 130 konton för att utföra bedrägerierna.
Bland de drabbade finns: Bill Gates, Elon Musk, Jeff Bezos, Kanye West, Warren Buffet, Uber, Apple.
Många användarkonton för aktörer inom kryptovaluta användes för att lura till sig bitcoin från ovetande utomstående Twitteranvändare.
Dessutom var det många verifierade användare, kändisar, myndighetspersoner och journalister som drabbades. Deras konton användes också för att lägga ut inlägg som skulle lura deras många följare att skicka bitcoin till bedragarna.
Totalt 118 000 dollar fick de in på 24 timmar.

Hur märkte de att de blivit hackade?
På Garmin upptäcktes intrånget när anställda började dela information och foton av krypterade/låsta datorer i systemet.
Strax efter detta förlorade företaget kontrollen över i stort sett alla system, det gick varken att ringa, maila eller komma in på deras hemsida.
Interna produktions - och nätverkssystem slogs ut.
Smartklockor, GPS-system inklusive vissa för piloter, slogs ut.
Det gick inte ens att nå kundtjänst, det tog 4 dagar för att återgå till normalt läge.

När det gäller Twitter blev de medvetna om intrånget när flertalet anställda upptäckt märkliga inloggningar de inte gjort och märkliga registrerade telefonsamtal, dessutom kunde de anställda som blivit lurade inte logga in på sina konton efter att den påstådda ”IT-supporten” hjälpt dem med att lösa just inloggningsproblem.
När företagets interna responsteam höll på med utredningen av dessa problem och uppgifter, började kryptovaluteaktörer att publicera märkliga inlägg som uppmanade personer att föra över bitcoin till ett visst konto för att få en fördel inom information angående placering av kryptovalutor.

Vad för åtgärder vidtogs?
Garmin nämnde inte attacken offentligt men efter 4 dagar började man återställa alla system med hjälp av en dekrypteringsnyckel, vilket ledde till misstankar att man betalat den begärda lösensumman för att få nyckeln av gärningsmännen. Enligt dessa misstankar fick Garmin hjälp av företaget Arete IR, varken Garmin eller Arete IR bekäftar dessa misstankar.
En annan uppgift från businessinsider.com gör gällande att ett annat företag först konsulterats som mellanhand för betalningen men att detta företag som vill vara anonymt, nekat att hjälpa till då det strider mot sanktionerna som finns mot Evil Corp, som ansågs ligga bakom intrånget.
Twitter raderade först märkliga inlägg och försökte låsa alla konton som hade koppling till intrånget medan de utredde vad om hänt. När det visade sig svårare än de först trodde, låste de alla konton som är verifierade användare och hade bytt lösenord inom 30 dagar.
Sedan fick alla anställda byta sitt lösenord med sin överordnade som vittne i videosamtal, från VDn hela vägen till vanliga anställda, innan allting återgick till det vanliga. Detta förfarande kallas för ”Zero Trust” och innebär att man inte litar på någon, för säkerhets skull.
För övrigt hindrades tusentals bitcoin-överföringar till bedragarna av kryptovaluta-aktören Coinbase till ett värde av cirka 280 000 dollar då bedragarens bitcoin-konto tidigt svartlistades av Coinbase.
Fjorton användare på Coinbase hann föra över totalt cirka 3000 dollar innan de satte stopp för fler överföringar. Det tog dem endast någon minut att upptäcka att något var fel.

Hur kommunicerades det ut till allmänheten?
Garmin lämnade ett pressmeddelande 4 dagar efter händelsen som bland annat tar upp att många onlinetjänster blev drabbade av störningar, inklusive hemsidefunktioner, kundtjänst, applikationer och kommunikation med företaget. De meddelar även att inga uppgifter om deras kunder har läckt ut utan att det endast drabbade deras funktioner.
Det tas inte upp något angående lösensumman eller hur de löste problemet.

Twitter meddelande initialt att man håller på med att radera bilder på deras interna kontohanteringsverktyg som av någon anledning dyker upp många olika bekräftade användares inlägg och även på konton kopplade till bitcoinbedrägeriet. Senare meddelade de att de var medvetna om att en säkerhetsincident som påverkar användares konton pågår och att de vidtar åtgärder som ska lösa problemet.

Diskussion

Vad hade företagen eventuellt kunna göra annorlunda?

Garmin hade troligtvis haft nytta av att ha ett backup-system så de hade sluppit att betala lösensumman till gärningsmännen. De hade också kunnat ha separerat på olika system så att inte allting blev drabbat av samma virus.
Dessutom vore det kanske bra om kundtjänst inte drabbas alls, då de kan svara på frågor och lugna kunderna och aktieägare.

Twitter stängde ner samtliga verifierade användare som hade bytt lösenord de senaste 30 dagarna, inklusive konton som tillhör samhällsviktiga funktioner. En av dessa var Tornadovarningar från väderlekstjänsten som inte kunde postas på Twitter medan de felsökte och försökte åtgärda problemet.
En lösning jag kan tänka mig är att samhällsviktiga funktioner ska ha prioritet framför andra användare så att de så snabbt som möjligt kan fortsätta med sin verksamhet.

Förslag på allmänna åtgärder och observationer:

Det finns mycket att lära av båda företagens agerande och det finns flera viktiga nyckelåtgärder som hade kunnat vidtagits för att förhindra båda attackerna.
Jag kommer att lista några av åtgärderna som jag själv som nybörjare inom IT-branschen känner kan vara mest aktuellt baserat på det jag läst och lärt mig hittills.

1.Ransomware-attacker är väldigt riktade emot de som kan vara intressanta måltavlor, framförallt företag som inte har råd att ha en verksamhet som ligger nere antingen ekonomiskt, verksamhetsmässigt eller av andra skäl, till exempel sjukhus. De riktas just emot de som har mängder av värdefull användardata som är beroende av att den finns online hela tiden. Det leder till att gärningspersoner eller organisationer kan ta ut en hög lösensumma eftersom att de vet att mycket står på spel.

2.Om det vore fallet att Garmin har betalat lösensumman, finns risken att de ses som en betalningsvillig måltavla och blir därmed ett attraktivt mål för framtida attacker, dessutom upptäcker gärningspersonerna att även fast det finns en sanktion riktad emot dem så kan de få betalt ändå. Tänker främst på Evil Corp som tidigare stulit cirka 100 miljoner dollar av banker och därmed var belagda av sanktioner och ändå i så fall fick betalt då man kringgår sanktioner via mellanhänder. Dessutom investerar ofta dessa kriminella sina intjänade pengar i att förfina verksamheten ännu mer, det blir en ond spiral.
Å andra sidan kan man hävda att hade Garmin inte betalat, då hade de aldrig fått igång verksamheten i tid och därmed tappat massvis med kunder.
För övrigt finns det allmänt ingen garanti för att gärningspersonerna ger dig dina filer tillbaka bara för att du betalar.

3. Många av RansomWare-attackerna är så sofistikerade när det gäller hur virusprogrammen är konstruerade och i dagsläget är det ofta svårt om inte omöjligt att dekryptera dem på egen hand. Ju mer cyberskurkarna utvecklar mer avancerade program, desto svårare blir det att avkoda deras virus.
Många gånger är det enda alternativet att betala och hoppas.
Det finns ett stort mörkertal om hur många företag som blivit drabbade och betalat i tysthet enligt många IT-säkerhetsexperter.

4. Tröskeln till katastrof är väldigt låg.
Det räcker med att en enda anställd har dålig koll på vad för email den öppnat eller länk den tryckt på, för att hela nätverket ska bli infekterat.

5.Att bli attackerad och att det kommer ut i allmänheten kan skada ens rykte som ett säkert företag. Det gäller att vidta nödvändiga säkerhetsåtgärder på alla plan.

Hur förhindrar man att bli attackerad och hur skademinimerar man eventuell attack?

1.Fokus på kunskap hos alla anställda.
Första försvarslinjen mot alla typer av nätfiskeattacker är kunnig personal.
Om man utbildar alla anställda regelbundet om vad man ska och inte ska göra på mailen och nätet har man en bra grund att börja med. Det finns övningsprogram och utbildningar mot nätfiske.
Håll regelbundna informationsmöten eller skicka information till de anställda om nya metoder som används för att göra intrång, exempelvis nya nätfiskemetoder.

2. Ha en eller flera experter på området beroende på företagets storlek.
Om man tränar upp interna IT-säkerhetsexperter som sedan kan utbilda de anställda vidare och hålla dem uppdaterade med information om de senaste hoten och hur man skyddar sig mot dem så ökar chansen till att upptäcka ett hot. Om personen dessutom kan skapa engagemang och vilja att verkligen ha en säker organisation är det en stor fördel för företaget.

3. Håll mjukvara och alla maskiner uppdaterade och moderna.
Om varenda dator på arbetsplatsen är modern och har senaste uppdateringarna så minskar risken för att någon utnyttjar ett kryphål i något system.
En gammal dator med Windows XP som slutade med säkerhetsuppdateringar för flera år sedan, som är inkopplad på företagets nät, är inget att rekommendera om man bryr sig om IT-säkerhet.

4.Gör som Twitter och begränsa vilka som har tillgång till administrativa verktyg, alla behöver inte vara SysAdmin för att utföra sitt dagliga arbete.

5. Ha en backup / säkerhetskopiera allt viktigt!
Om ni som företag har säkerhetskopierat era uppgifter med jämna mellanrum kan ni be eventuella hackare att söka sig annorstädes eftersom deras utpressningsförsök blir tandlöst om ni bara behöver ladda upp allting på nytt.
Då sponsrar ni inte bedragare, ni klarar er om systemet kraschar av andra anledningar och visar utåt att ni är ett modernt företag som kan hantera kriser.

Källförteckning

Källor anges under rubriken Bakgrund,

Bilagor

Inga bilagor att bifoga.

Figur- och tabellförteckning

Ej med i denna rapport.