DELL Technologies

Lärdomar från en utpressningsprogramattack

på Universitat Autònoma de Barcelona

Gonçal Badenes
CIO, Universitat Autònoma de Barcelona.
Intervjun har förkortats och redigerats för tydlighetens skull.

Snabba åtgärder, transparens och ett förnyat engagemang för att uppdatera cybersäkerheten definierade universitetets svar på en utpressningsprogramattack.

Sameer Shah, Dell Technologies Cybersecurity Marketing, pratade med CIO Gonçal Badenes om incidenten.

Shah: Vi har pratat om behovet av att hjälpa organisationer att stegvis öka cybersäkerheten. Ni drabbades alla av en cyberattack för ett tag sedan. Innan vi går in mer i detalj på attacken, kan du berätta lite om universitetet och dess IT-miljö?

Badenes: Universitat Autònoma de Barcelona är ett av de ledande universiteten i Spanien. IT övervakar alla tjänster som behövs för att driva universitetet.

Strax före attacken hade vi en detaljerad plan för att förbättra cybersäkerheten. Vi hade driftsatt flerfaktorsautentisering (MFA), men inte för alla tjänster och användare. Studenter och all IT-personal hade redan MFA men bara på Microsoft 365-plattformen. Andra tjänster skyddades inte. Avsaknaden av universell MFA var avgörande, vilket vi skulle märka senare.

När inträffade attacken och vilken typ av attack var det?

Det var en utpressningsprogramattack som inträffade under en långhelg, vilket vanligtvis är fallet. Vid fyratiden på morgonen fick jag ett samtal från mitt team som sa att det var tjänster som gick ner som dominobrickor. De slog larm och vi satte omedelbart ihop det insatsteam som vi hade satt ihop för den här typen av fall.

Hur visste du att det rörde sig om en utpressningsprogramattack? Fanns det ett krav på lösensumma?

Det fanns krav på lösensumma på de system som påverkades. Men de genomförde också en mindre attack genom att köra ett skript för att kryptera datorer som var online under helgen. Effekten av det var begränsad och huvudsyftet var förmodligen att se till att personalen och studenterna fick reda på attacken, inte bara IT-teamet.

Övervägde din organisation vid något tillfälle att betala lösensumman?

Nej.

Varför inte?

Vi kunde inte göra det ur en etisk synvinkel. Som tur var hade vi säkerhetskopior, två kopior i två olika datacenter på campus och en tredje på band utanför organisationens område.

Och för att vara tydlig, dessa säkerhetskopior var inte ett datavalv?

Nej, inte just då. Vi hade inget valv. Det var en framtida prioritering i handlingsplanen. Men sedan prioriterades det förstås [efter attacken].

Kommunikation kan vara avgörande i dessa situationer. Det låter som att du fick ett övertag under attacken genom att kommunicera tydligt och transparent, även med media?

Ja, från dag ett. Vi var tvungna att vara helt transparenta och öppna och förklara vad som hade hänt. Vi såg till att andra människor kunde förbereda sig och lära sig av vår erfarenhet. Min gissning är att en del av pressen faktiskt läste utpressningsbrevet och kontaktade angriparna eftersom vi aldrig gjorde det. Angripargruppen identifierade sig som PISA-gruppen (Protect Your System, Amigo).

Många gånger föredrar organisationer sekretess för att undvika att exponera sina svagheter eller åtgärdstaktik. Var det något ni övervägde?

Det där är befogade farhågor. Men jag är ganska säker på att vi alla vet att vi är sårbara. När vi försöker säkra vårt hem vet vi att även om vi köper den bästa dörren på marknaden kommer inbrottstjuvar som vill ta sig in att hitta ett sätt att bryta upp den eller hitta ett annat sätt att komma in. Det är exakt samma sak här.

Det finns ingen skam i det faktum att vi attackerades och hade sårbarheter. Det faktum att vi hade en mycket tydlig handlingsplan för skydd och ändå drabbades är viktigt att berätta om. Även om vi hade ett mycket bra skydd hade vi fortfarande sårbarheter som kunde attackeras. Genom att implementera ytterligare steg kan du stärka din position ännu mer.

Berätta vad du gjorde först för att börja ta itu med problemet.

Vi stängde ner nätverket, alla system. Vi kontaktade polisen och den regionala myndigheten för dataskydd, vilket är saker som vi måste göra enligt lagen. Då startade vi omedelbart två team: kriminalteknik och återställning. Vi ringde Dell och ärendet eskalerades omedelbart till högsta prioritet, och vi fick ett fantastiskt team som arbetade med det oavbrutet. De lyckades helt återställa all data på den andra datadomänen.

Så kriminalteknikteamet påbörjade sitt arbete under återställningsprocessen?

För vissa av återställningsprocesserna var vi tvungna att vänta lite. Det är därför jag säger att kriminalteknikteamet började först. Allt sattes i karantän eftersom vi först måste förstå vad som hade hänt. Vi var tvungna att sätta ihop ett annat system så att vi kunde börja sätta igång saker igen. Vi bestämde oss för att alla system som skulle komma online behöver uppfylla de bästa standarderna inom säkerhet, även om det skulle ta lite längre tid.

”Jag tror att det viktigaste att tänka på är att det finns en stor sannolikhet för att vi alla förr eller senare kommer att drabbas av en cyberattack och att vi därför måste ha en klar detaljerad plan för begränsning och återställning.”

Du nämnde att MFA endast fanns på Microsoft 365, vilket var en del av det som möjliggjorde attacken. Så, har ni MFA överallt nu?

Attackvektorn var en användare med komprometterade inloggningsuppgifter som var med i ett team som redan hade MFA på Microsoft. Men när angriparen försökte komma åt e-postadressen och såg att de inte kunde komma åt det på grund av MFA fortsatte de att söka. Och de fick reda på att vi har en VPN som inte var skyddad av MFA. När de väl fick tillgång via VPN kunde de börja kartlägga nätverket.

I ett sådant stort nätverk som vårt hittade de ett system som hade en sårbarhet och började röra sig i sidled. Så nu, när vi började återställa systemen, bestämde vi oss för att ingenting skulle komma online förrän det var skyddat med MFA.

Om du kan ge dina kollegor EN viktig rekommendation eller ETT råd för att undvika en utpressningsprogramattack, vad skulle det vara?

Det är svårt att ge ett enda råd, men jag tror att det viktigaste att tänka på är att det finns en stor sannolikhet för att vi alla förr eller senare kommer att drabbas av en cyberattack och att vi därför måste ha en klar detaljerad plan för begränsning och återställning.

Det är till exempel mycket viktigt att ha kontaktuppgifterna till viktiga partner inom kriminalteknik och återställning till hands och att ha en detaljerad och prioriterad karta över tjänster med en tidslinje för återställning. Dessutom är det viktigt att ha en väl anpassad strategi med de viktigaste affärsenheterna, däribland kommunikation (både intern och extern). Och det är naturligtvis mycket viktigt att se till att användarna är uppmärksamma och utbildade om de tekniker som används av angripare.

Känner du att förstärkningen av cybersäkerheten vid universitetet har ökat förtroendet för att ni ska kunna fortsätta uppdraget och göra fantastiska saker?

Absolut! Före attacken var en av uppfattningarna att alla nya åtgärder för att skydda systemet mottogs med många frågor och farhågor om huruvida vi verkligen behöver dem. Faktum är att skydd är absolut nödvändigt. Annars sätter du hela ditt företag i fara. Det finns naturligtvis fortfarande de som anser att dessa åtgärder hindrar deras arbete. Men de flesta anser att systemen är mycket bättre skyddade.

Tack. Din uppriktighet och transparens är fördelaktig för alla som arbetar för att förbättra sin cybersäkerhet.