Platformele de comunicare online, bazate pe cloud, si riscurile în fata atacurilor cibernetice (analiza Eset)

Solutiile de comunicare online, bazate pe cloud, precum Microsoft Teams, Slack si Zoom, au devenit populare odata cu izbucnirea pandemiei de COVID-19, însa în acelasi timp popularitatea acestora a atras, dupa sine, si interesul hackerilor, sunt de parere expertii Eset, producatorul de solutii de securitate IT.

Potrivit unei analize, publicate recent, atacurile cibernetice în cloud au reprezentat 20% din toate incidentele de acest fel, numai în 2020.

"Deoarece popularitatea serviciilor bazate pe cloud nu a scazut, nici interesul atacatorilor nu se clatina. Daca ne uitam la cele trei platforme mentionate mai sus, putem identifica o tendinta: aplicatiile concepute în principal pentru munca si colaborare au fost transformate, prin comportamentul utilizatorilor, în platforme de comunicare si interactiune sociala", sustin specialistii.

Analiza de specialitate evidentiaza faptul ca, în prezent, Microsoft Teams, lansata în 2017, este aplicatia Microsoft cu cea mai rapida crestere si a devenit instrumentul de comunicare preferat de catre multi utilizatori. Numarul anual de utilizatori ai aplicatiei aproape ca s-a dublat între anii 2020 si 2021, iar în 2022, utilizatorii au atins un numar de 270 de milioane, dintre care majoritatea sunt în categoria de vârsta activa (35-54 de ani).

Pe fondul acestui interes, Microsoft Teams nu este lipsita de riscuri, iar în 2021 în aplicatie a fost descoperita o vulnerabilitate care a permis persoanelor rau intentionate sa primeasca acces în conturi si sa fure e-mailuri, mesaje din aplicatia Teams si fisiere din OneDrive si SharePoint.

"Mai recent, în august 2022, a fost descoperita o noua vulnerabilitate: din cauza faptului ca Teams stoca token-urile de acces pe disc, acestea erau mai usor de furat în cazul în care un atacator reusea sa compromita un computer slab protejat, transformându-l în punct de acces. Pentru unii dintre utilizatori, aceste puncte slabe indica faptul ca solutiile bazate pe cloud sunt mai susceptibile la atacuri decât cele instalate local si, prin urmare, au nevoie de un strat special de protectie bazat pe cloud", se mentioneaza în documentul Eset.

Conform datelor citate, o alta solutie bazata pe cloud pentru videoconferinte si care a devenit un nume cunoscut în ultimii ani este Zoom, platforma software "peer-to-peer" care parea a fi optiunea perfecta, deoarece nu necesita existenta unui cont pentru a participa la un eveniment.

"Bineînteles, utilizarea pe scara larga a Zoom a devenit un punct de interes pentru profesionistii din domeniul securitatii IT si pentru actorii rau intentionati deopotriva. Din 2020, platforma a intrat în centrul atentiei de mai multe ori, inclusiv pentru probleme de confidentialitate si securitate care nu au fost create de aceasta. Într-o situatie larg mediatizata, fostul prim-ministru britanic Boris Johnson a fost criticat pentru ca a dezvaluit din greseala un ID de sedinta Zoom pentru o reuniune a cabinetului, ceea ce a stârnit îngrijorari cu privire la faptul ca sedintele au fost expuse unui risc sporit de spionaj si de atacuri cunoscute sub numele de Zoombombing. De asemenea, la începutul pandemiei, hackerii au adunat peste 500.000 de nume de utilizator si parole Zoom printr-un atac cunoscut sub numele de "credential stuffing", înainte de a publica datele obtinute pe dark web", subliniaza expertii.

O alta problema de securitate asociata cu platforma a implicat vulnerabilitati de securitate, inclusiv una care a afectat aplicatia Zoom pentru macOS si care ar fi putut oferi hackerilor acces de tip "admin" la desktopurile macOS, dupa care, la începutul anului 2022, echipa Project Zero de la Google a dezvaluit o depasire de "buffer" si o vulnerabilitate ce ar fi putut facilita scurgerea de informatii din Zoom care, înainte de a fi remediata, ar fi putut permite infractorilor cibernetici sa monitorizeze sedintele Zoom.

În acelasi timp, aplicatia destinata comunicarii si productivitatii, Slack, care pretinde ca reduce nevoia de e-mailuri cu 32% si de sedinte cu 27%, este o victima a propriului sau succes, dupa cum afirma reprezentantii Eset. Astfel, aplicatia folosita de peste 100.000 de organizatii din întreaga lume, prezinta, la rândul ei, o serie de vulnerabilitati si riscuri pentru utilizatori.

"O vulnerabilitate mai recenta a fost raportata în 2019. Aceasta a permis atacatorilor sa exploateze o slabiciune în Slack Desktop pentru Windows prin modificarea locului în care erau descarcate fisierele trimise prin intermediul unui canal Slack. Astfel, infractorii au reusit sa injecteze malware în fisiere sau chiar sa le fure. Aceasta, desigur, nu este prima problema de securitate, fiind descoperite si alte vulnerabilitati majore înca din 2015. Unul dintre cele mai evidente dezavantaje ale Slack pare sa fie functia sa de tip comunitati deschise, care permite conectarea unor grupuri mari de persoane. La fel ca si e-mailul, Slack a devenit un vector perfect pentru phishing si spam", se noteaza în analiza.

Eset a fost fondata în anul 1992 în Bratislava (Slovacia) si se situeaza în topul companiilor care ofera servicii de detectie si analiza a continutul malware, fiind prezenta în peste 180 de tari.