Bulut havfsizlik nima?

Bulut Xavfsizlik Ta'riflangan, Ta'riflangan va Tadqiqlangan



Bulut havfsizligi belgilandi

Bulutli hisoblash xavfsizligi deb ham ataladigan bulutli xavfsizlik, bulutli tizimlar, ma'lumotlar va infratuzilmani himoya qilish uchun birgalikda ishlaydigan siyosatlar, boshqaruvlar, protseduralar va texnologiyalardan iborat. Ushbu xavfsizlik choralari ma'lumotlarni himoya qilish, tartibga rioya qilishni qo'llab-quvvatlash va mijozlarning shaxsiy hayotini himoya qilish hamda alohida foydalanuvchilar va qurilmalar uchun autentifikatsiya qoidalarini belgilash uchun tuzilgan. Havfsiz trafikni kirish uchun autentifikatsiya qilishdan bulutli xavfsizlik biznesning aniq ehtiyojlariga moslashtirilishi mumkin. Va bu qoidalar bir joyda konfiguratsiya va boshqarilishi mumkinligi sababli, ma'muriy xarajatlar kamayadi va AT komandalari biznesning boshqa sohalariga e'tibor berishga qodir.

Bulutdagi xavfsizlikning yetkazib berilishi bulutli provayderga yoki bulutdagi xavfsizlik echimlariga bog'liq bo'ladi. Biroq, bulutli xavfsizlik jarayonlarini amalga oshirish biznes egasi va hal provayderi o'rtasida umumiy mas'uliyat bo'lishi kerak.

Nima uchun Cloud Xavfsizlik muhim?

Bulutga o'tishni amalga oshiradigan korxonalar uchun mustahkam bulutli xavfsizlik talab qilinadi. Xavfsizlik tahdidlari doimo rivojlanib bormoqda va murakkablashib bormoqda, va bulutli hisob-kitoblar mahalliy sharoitga qaraganda xavf ostida emas. Shu sababli, infratuzilmangiz uchun moslashtirilgan eng yaxshi xavfsizlik ta'minlovchi bulut provayderi bilan ishlash juda muhimdir.

Bulutli xavfsizlik ko'p foyda beradi, jumladan:

Markazlashtirilgan xavfsizlik: bulutli hisoblash dastur va ma'lumotlar markazlashtirgandek, bulutdagi xavfsizlik xavfsizlikni markazlashtiradi. Bulutli biznes tarmoqlari ko'plab qurilmalardan va so'nggi nuqtalardan iborat. Ushbu korxonalarni boshqarish trafikni tahlil qilish va filtrlashni markazlashtirilgan tarzda yaxshilaydi, tarmoq voqealari monitoringi jarayonini tartibga soladi va natijalar dasturiy ta'minot va siyosat yangilanishlarini kamaytiradi. Tabiiy ofatlarni tiklash rejalari ham bir joyda boshqarilganda osonlik bilan amalga oshirilishi va amal qilishi mumkin.

Kam xarajatlar: bulutli saqlash va xavfsizlikni qo'llashning afzalliklaridan biri - bu maxsus uskunalarga investitsiyalar kiritish zarurligini bartaraf etishdir. Bu nafaqat kapital xarajatlarni kamaytiradi, balki u ma'muriy xarajatlarni kamaytiradi. AT komandalari xavfsizlik masalalari tezkor ravishda yong'in xavfsizligi bilan shug'ullangan bo'lsa, bulutli xavfsizlik xavfsizlikni ta'minlovchi proaktiv xususiyatlarni taqdim etadi.

Azaltilgan ma'muriyat: Siz taniqli bulut xizmatlarini ko'rsatuvchi provayderni yoki bulutli xavfsizlik platformasini tanlaganingizda qo'lda xavfsizlik konfiguratsiyasi va deyarli doimiy xavfsizlik yangilanishlari bilan xayrlashuvni o'stirishingiz mumkin. Ushbu vazifalar resurslarga katta miqdorda drenaj berishi mumkin, lekin ularni bulutga ko'chirsangiz, barcha xavfsizlik idoralari bir joyda bo'ladi va sizning nomingizdan to'liq boshqariladi.

Ishonchlilik: Cloud computing xizmatlari ishonchliligi bilan yakunlanadi. To'g'ri bulutli xavfsizlik choralarini qo'llagan holda, foydalanuvchilar qaerda bo'lishidan qat'i nazar, qaysi qurilma yoki qaysi qurilma ishlatilayotganidan qat'i nazar, bulut ichida ma'lumotlarni va ilovalarni xavfsiz tarzda olishlari mumkin.

Ko'plab tashkilotlar o'z tizimlarini bulutga ko'chirishning ko'pgina biznes afzalliklarini ro'yobga chiqarmoqda. Cloud computing korxonalar miqyosida ishlashga, texnologiya xarajatlarini kamaytirishga va ularga raqobatbardoshlikni ta'minlaydigan tezkor tizimlarni ishlatishga imkon beradi. Biroq, tashkilotlarning bulutli hisoblash xavfsizligiga to'liq ishonishlari va barcha ma'lumotlar, tizimlar va ilovalar ma'lumotlarni o'g'irlash, qochish, korruptsiya va o'chirishdan himoyalangan bo'lishi juda muhimdir.

Barcha bulutli modellar tahdidlarga moyil. IT bo'limlari bulutga muhim tizimlarni ko'chirishga nisbatan ehtiyotkorlik bilan qarashadi va siz mahalliy bulut, gibrid yoki mahalliy muhitda ishlayotgan bo'lsangiz ham, to'g'ri xavfsizlik qoidalari zarur. Bulutli xavfsizlik an'anaviy IT xavfsizligining barcha funktsiyalarini taklif qiladi va korxonalar bulutli hisoblashning ko'pgina afzalliklarini ishlatish imkonini beradi va xavfsizligini ta'minlaydi va shuningdek, ma'lumotlar maxfiyligi va moslik talablariga javob berishini ta'minlaydi.

To'g'ri bulutli xavfsizlik echimini tanlash

Agar bulutdan eng yaxshisini olishni istasangiz va tashkilotingiz ruxsatsiz kirishdan, ma'lumotlar buzilganidan va boshqa tahdidlardan himoyalanganligini bilmoqchi bo'lsangiz, biznesingiz uchun to'g'ri bulutli xavfsizlik echimini tanlash kerak. Forcepoint Cloud Access havfsizlik Broker (CASB) bulutli ilovalarni va ma'lumotlarni himoya qiluvchi to'liq xavfsizlikni ta'minlovchi yechim bo'lib, buzilgan hisoblarni to'sadi va har bir qurilmada xavfsizlik siyosatini o'rnatish imkonini beradi. Natijada, ma'lum va paydo bo'layotgan tahdidlardan to'liq himoyalangan bulutli infratuzilma va sizning tashkilotingiz bulutli hisoblashning eng yaxshi usullaridan foydalanishga imkon beradi.

Bulut havfsizlik

JAKE FRANKENFIELD tomonidan ko'rib chiqildi

Cloud Xavfsizlik nima o'zi

Bulutli xavfsizlik - bu o'g'irlik, qochish va o'chirishdan onlayn tarzda saqlangan ma'lumotlarning muhofazasi. Bulutli xavfsizlikni ta'minlash usullari orasida xavfsizlik devorlari, penetratsion sinovlar, obfuscation, tokenization, virtual xususiy tarmoqlar (VPN) va internetga ulanishning oldini olish kiradi. Bulutli xavfsizlikka nisbatan asosiy tahdidlar ma'lumotlar buzishlar, ma'lumotlarning yo'qolishi, hisobni o'g'irlash, xizmatni tashish qobiliyatini yo'qotish, xavfli dastur dasturi interfeyslari (API), bulutli saqlash xizmatlarining yomon tanlovi va bulutli xavfsizlikni buzadigan umumiy texnologiyalardir. Tarqatilgan rad etish xizmati (DDoS) hujumlari bulut havfsizligiga yana bir tahdiddir. Ushbu hujumlar foydalanuvchilarning o'z hisoblariga, masalan, bank hisoblari yoki elektron pochta hisoblariga kira olmasliklari uchun xizmatni o'chirib yuboradi.

Pastdagi bulut havfsizlik

Bulutda saqlaydigan ma'lumotlarning xavfsizligi haqida tashvishlanayotgan ko'plab foydalanuvchilar uchun bu xavfsizlik ta'minoti zarur. Ular o'z ma'lumotlarini o'zlarining mahalliy serverlarida xavfsizroq deb hisoblashadi, chunki ular o'zlarining ma'lumotlar ustidan ko'proq nazoratga ega ekanligini his qilishadi. Ammo bulutda saqlanadigan ma'lumotlar aslida yanada xavfsiz bo'lishi mumkin, chunki bulutli xizmat ko'rsatuvchi provayderlar ustun xavfsizlik choralariga ega va ularning xodimlari xavfsizlik mutaxassislari. Tashkilotdagi ma'lumotlar xavfsizlikka ziyon etkazishi mumkin, hujum turiga qarab. Ijtimoiy muhandislik va zararli dasturiy ta'minot har qanday ma'lumotlarni saqlash tizimini zaiflashtirishi mumkin, lekin saytdagi ma'lumotlar xavfsizlik nuqtai nazaridan kamroq tajribaga ega bo'lganligi sababli, saytdagi ma'lumotlar yanada himoyasiz bo'lishi mumkin.

Bulutli xavfsizlik - bu bulutli saqlash provayderlari uchun asosiy muammo. Ular nafaqat mijozlarini qoniqtirishlari kerak; ular kredit karta raqamlari va sog'liqni saqlash ma'lumotlari kabi nozik ma'lumotlarni saqlash uchun muayyan tartibga solish talablariga rioya qilishlari kerak. Bulut provayderining xavfsizlik tizimlari va protseduralarining uchinchi taraf auditi foydalanuvchining ma'lumotlarining xavfsizligini ta'minlashga yordam beradi.

Bulutdagi ma'lumotlarning xavfsizligini ta'minlash bulutning o'zini ta'minlashdan tashqarida. Bulutli foydalanuvchilar mobil qurilmalarda saqlangan ma'lumotlardan yoki login hisob ma'lumotlari bilan beparvo bo'lishdan olinadigan bulutga kirishni himoyalashi kerak. Boshqa bulutli xavfsizlik muammosi, boshqa mamlakatlarda joylashtirilgan bulutda saqlangan ma'lumotlarning turli qoidalarga va maxfiylik choralariga ta'siri bo'lishi mumkin.

Agar bulutli provayderni tanlashda, fon tekshiruvlari va xavfsizlik vositalari orqali yomon niyatli shaxslardan himoyalanishga harakat qiladigan kompaniya tanlash muhimdir. Aksariyat odamlar tashqi xakerlar bulut havfsizligi uchun eng katta tahdid deb hisoblashadi, lekin xodimlar katta xavf ostida. Ushbu xodimlar, albatta, zararli insider emas; ular odatda bilmagan holda kompaniyaning o'z tarmog'i xavfsizligiisiz nozik kompaniya ma'lumotlariga kirish uchun shaxsiy smartfondan foydalanish kabi xatolarga yo'l qo'yadigan xodimlardir.

9 Cloud Computing havfsizlik har bir kompaniyaning yuziga xavf soladi

Sizning ma'lumotingizni himoya qilish uchun qanday qadamlar kerak

Forrester tahlil firmasi ma'lumotlariga qaraganda, 2020 yilga borib 91 milliard dollarni tashkil etadigan jahon miqyosidagi bulutli hisoblash bozorining 2020 yilgacha 191 milliard dollargacha o'sishi kutilmoqda. Bulutli hisob-kitoblar bulutga sekulyar o'tishni ta'minlovchi ko'pgina afzalliklari mavjud; ular orasida arzon narx, bozorga tezroq kirish va xodimlarning unumdorligini oshiradi. Ammo, bulutdagi ma'lumotlarning xavfsizligi AT-bo'limlari uchun bulutni qabul qilishni va CASBni qabul qilishni boshqarishda muhim ahamiyatga ega. Xodimlar ITni kutishmaydi; bulut xizmatlarini "o'zingizning bulutingizni" yoki "BYOC" harakatini kengaytirishning bir qismi sifatida ishlashga taklif qilmoqda. Ponton instituti 400 ta IT va IT xavfsizligi rahbarlarini kompaniyalarning foydalanuvchilar tomonidan boshqariladigan bulutlarni qabul qilishni qanday boshqarayotganlarini aniqlash uchun so'radi.

Pemon ishi 9 ta bulut xavfini aniqladi. Evernote platformasi, Adobe Creative Cloud, Slack va LastPass bulut platformalaridagi yuqori darajadagi buzilishlar ortidan AT bo'limlari qiziqtirmaydi. LastPass buzilishi ayniqsa, bezovtalanmoqda, chunki xizmat foydalanuvchining veb-saytini va bulut xizmatining parollarini saqlaydi. Ushbu parollar bilan qurollangan, ayniqsa, kompaniyaning muhim infrastrukturasi uchun keng ko'lamli ruxsatnomalarga ega bo'lgan boshqaruvchilarga tegishli bo'lganlar, kiber-kriminalizatsiya dahshatli hujumni boshlashi mumkin. Buzilish miqyosi keng va 91% kompaniyaning kamida bitta LastPass foydalanuvchisi mavjud. Ushbu kompaniyalardagi IT-bo'linmalari LastPass yordamida ishlaydigan xodimlar ham borligini bilishmaydi.

So'nggi bir necha yil ichida odamlar uchun yanada samarali bo'lishiga yordam beruvchi yangi ilovalar portlashi yuz berdi. Xodimlar bu ilovalarni o'zlari bilan ishlash uchun yanada samarali ishlash uchun jalb qilmoqda. Ilgari fikrlaydigan kompaniyalar o'zlarining tashkilotlari uchun o'zingizning bulutingizni (BYOC) harakatini keltirib chiqarishning afzalliklarini bilishar ekan, siz buni "shadow IT" ning eng dahshatli nomi deb atashingiz mumkin. Ko'p holatlarda, Soya IT yaxshi niyat bilan boshlanadi. Xodimlar korporativ ma'lumotni xavfsiz bo'lmagan ilovalarda saqlashi mumkin bo'lgan xatarlardan xabardor bo'lmagan holda, ularning ishlarida yaxshi bo'lishiga yordam beradigan ilovalardan foydalanadi. Skyhigh 18 million ishchini bulutdan foydalanishni tahlil qildi va o'rtacha kompaniya 923 bulut xizmatidan foydalanishini aniqladi.

Tadqiqot 409 IT va xavfsizlik rahbarlari, Pemon Institute nashri o'z bulutingizni olib kelish xavfi (BYOC) bulut xizmatining xavfini o'rganib chiqdi. So'rov natijalariga ko'ra, respondentlarning ko'pchiligi BYOC tashkilotining muammolari qanchalik keng tarqalganligini bilishmaydi. Ular qanday ilovalar va bulutli xizmat xodimlari ishlayotganini bilishmaydi va bundan ham yomoni, ular qanday ma'lumotlarga duch kelayotganini, qaerga ketayotgani va kim bilan o'rtoqlashayotganini bilmaydi. So'rovda respondentlar tomonidan aniqlanganidek, BYOC-ning eng katta xavfi mavjud. Ushbu xatarlarning ba'zilari xizmatlarning zaif bulutli xavfsizlik choralari bilan bog'liq, masalan, ma'lumotlarni shifrlash kabi ma'lumotlarni saqlash yoki xizmatga kirish uchun ko'p faktoring autentifikatsiyasining yo'qligi kabi ma'lumotlarni saqlash.

1. Intellektual mulkni yo'qotish yoki o'g'irlash

Kompaniyalar tobora sezilarli ma'lumotlarni bulutda saqlaydi. Skyhigh tomonidan tahlil qilinadigan bo'lsak, bulutli fayl almashish xizmatlariga yuklangan fayllarning 21 foizi intellektual mulk, shu jumladan, nozik ma'lumotlarni o'z ichiga olgan. Agar bulut xizmati buzilgan bo'lsa, kiber jinoyatchilar bu nozik ma'lumotlarga kirishlari mumkin. Agar qoidabuzarlik bo'lmasa, ba'zi xizmatlar, agar ularning shartlari va shartlari ularga yuklangan ma'lumotlarga egalik qilishni talab qilsa, xavf tug'dirishi mumkin.

2. Tuzatish qoidalarini buzish va tartibga solish

Bugungi kunda aksariyat kompaniyalar shaxsiy ma'lumotlarini HIPAA, FERPA maxfiy talaba qaydlari yoki boshqa ko'plab hukumat va sanoat qoidalaridan biri kabi o'zlarining ma'lumotlarini tartibga solish bo'yicha nazorat ostida faoliyat yuritmoqdalar. Ushbu mandatlar bo'yicha kompaniyalar ma'lumotlarining qaerdaligini, kimga kirish imkoniyatiga ega ekanligini va qanday himoyalanayotganligini bilishi kerak. BYOC odatda ushbu qoidalarning har birini buzadi, bu tashkilotni jiddiy oqibatlarga olib kelishi mumkin bo'lgan holatga keltiradi.

3. Yakuniy foydalanuvchilar harakatlarini nazorat qilishni yo'qotish

Kompaniyalar bulutli xizmatlardan foydalanib, ishchilar haqida zulmatda bo'lganlarida, bu ishchilar juda ko'p narsalarni qila olishadi va hech kim bilmaydi - bu juda kech bo'lmasdan. Misol uchun, kompaniyadan iste'foga chiqadigan sotuvchi barcha mijozlar kontaktlari haqida hisobotni yuklab olishi, ma'lumotni shaxsiy bulutli saqlash xizmatiga yuklashi va u ma'lumotni raqobatchidan foydalanganidan so'ng olishlari mumkin. Yuqoridagi misol aslida bugungi kunda keng tarqalgan ichki xavflarning biri hisoblanadi.

4. Maqsadli hujumni boshlaydigan zararli dasturiy ta'minot

Bulutli xizmatlar ma'lumotlarni eksfiltratsiya vektori sifatida ishlatilishi mumkin. Skyhigh, yangi ma'lumotlar eksfiltratsiya texnikasini ochib tashladi, bu bilan hujumchilar nozik ma'lumotlarni video fayllarga kodladilar va ularni YouTube-ga joylashtirdi. Bundan tashqari, biz bir vaqtning o'zida 140 ta maxsus belgidan maxsus Twitter hisobiga nozik ma'lumotlarni exfiltratsiya qilgan zararli dasturlarni aniqladik. Dyre zararli dastur variantida kiber jinoyatchilar zararli dasturlarni fishing hujumlari yordamida maqsadlarga etkazish uchun fayl almashish xizmatlaridan foydalanganlar.

5. Mijozlar yoki biznes hamkorlar bilan tuzilgan shartnoma qoidalari buzilgan

Ishbilarmonlar o'rtasida tuzilgan shartnomalar ko'pincha ma'lumotlarning qanday ishlatilishini cheklaydi va kimga ruxsat berilishi mumkin. Ishchilar ruxsatisiz cheklangan ma'lumotlarni bulutga ko'chirishganda, biznes shartnomalari buzilishi va huquqiy choralar ko'rilishi mumkin. Xizmatga yuklangan barcha ma'lumotlarni o'z shartlari bo'yicha uchinchi tomon bilan bo'lishish huquqini o'zida mujassam etgan bulut xizmatining misolini ko'rib chiqing, shunda kompaniya biznes sherigi bilan tuzilgan maxfiylik shartnomasini buzadi.

6. Mijozlarning ishonchi kamaydi

Ma'lumotlarning buzilishi muqarrar ravishda mijozlar ishonchini kamaytiradi. Hech qachon to'lov karta ma'lumotlarini buzib kelayotgan birida, kiber jinoyatchilar maqsadidan 40 milliondan ziyod mijozlar krediti va debet kartalari raqamlarini o'g'irlagan. Ushbu buzg'unchi mijozlarga maqsadli do'konlardan uzoqlashishga olib keldi va kompaniya uchun biznesni yo'qotdi, natijada kompaniya daromadiga ta'sir ko'rsatdi. Quyidagi 9 raqamga qarang.

7. Jabrlanganlarga xabar berishni va xabar berishni talab qiluvchi ma'lumotlarni buzish

Agar sezgir yoki tartibga solinadigan ma'lumotlar bulutga qo'yilsa va buzilish sodir bo'lsa, kompaniyadan buzilishini oshkor qilish va potentsial qurbonlarga bildirishnoma yuborish talab qilinishi mumkin. Sog'liqni saqlash sohasida HIPAA va HITECH kabi ayrim qoidalar va Evropa Ittifoqining Ma'lumotlarni muhofaza qilish bo'yicha Direktivi ushbu tushuntirishlarni talab qiladi. Qonuniy jihatdan majburiy bo'lgan buzilishlarni oshkor qilgandan so'ng, regulyatorlar kompaniyaga qarshi jarimalar to'lashi mumkin, va bu ma'lumotlar da'volarni ko'rib chiqish uchun buzilgan iste'molchilar uchun odatiy hol emas.

8. Xaridorlarni ko'paytirish

Mijozlar ma'lumotlarining korporativ darajadagi xavfsizlik nazorati tomonidan to'liq himoyalanmaganligiga shubha qilsa, ular o'z bizneslarini ishonchli kompaniya uchun boshqa joyga olib ketishlari mumkin. Tanqidchilarning tobora o'sib borayotgan qo'shiqlari iste'molchilarga mijozlarning shaxsiy hayotini himoya qilmaydigan bulut kompaniyalaridan qochishlarini o'rgatmoqda.

9. Daromad yo'qotishlarni

Maqsadli ma'lumotlarning buzilishi haqidagi xabarlar sarlavhalar va ko'plab iste'molchilar maqsadli do'konlardan band bo'lgan dam olish mavsumida uzoqlashib, kompaniyaning har chorakdagi daromadining 46 foizga pasayishiga olib keldi. Kompaniya qiymati 148 million dollarni tashkil qilgan. Natijada, CIO va CEO iste'foga chiqdi va ko'pchilik kiber xavfsizlik dasturlari bo'yicha direktorlar kengashi tomonidan nazoratni kuchaytirilishini talab qilmoqda.

Ponemon BYOC tadqiqotiga ko'ra, respondentlarning aksariyati (64 foiz) o'z xodimlarining ish joylarida o'z bulutlaridan foydalanayotganlarini tasdiqlay olmaydilar. Bizni ishon, ular. Boshqarilmaydigan bulutlardan foydalanish xavfini kamaytirish uchun, kompaniyalar birinchi navbatda ularning xodimlari tomonidan ishlatiladigan bulut xizmatlariga ko'rinishi kerak. Ular qanday ma'lumotlarning qaysi bulut xizmatlariga va kim tomonidan yuklanganligini tushunishlari kerak. Ushbu ma'lumotlarga ko'ra, AT komandalari korporativ ma'lumotlar xavfsizligini, muvofiqligini va boshqaruv tamoyillarini bulutdagi korporativ ma'lumotlarni himoya qilishni joriy qilishni boshlashi mumkin. Bulut bu erda qoladi va kompaniyalar bulut xizmatlarining xatarlarini muvozanatlashishi kerak, ular keltiradigan aniq foydalar bilan.

Gartner o'zining tadqiqot nashrlarida tasvirlangan mahsulot, xizmat yoki xizmatni qo'llab-quvvatlamaydi va texnologiya foydalanuvchisiga faqatgina eng yuqori reytingga yoki boshqa belgilarga ega bo'lgan sotuvchilarni tanlashga maslahat bermaydi. Gartner tadqiqot nashrlar Gartner tadqiqot tashkilotining fikrlaridan iborat bo'lib, aslida bayonot sifatida talqin qilinmasligi kerak. Gartner ushbu tadqiqot bo'yicha, sotish yoki muayyan maqsadga muvofiqligini kafolatlaydigan barcha kafolatlarini rad etadi.