jamf

Beveiliging 360:
jaarlijks trendrapport

Inleiding

Vorig jaar onderzochten we hoe de toepassing van technologieën op afstand de beveiligingshouding van bedrijven wereldwijd beïnvloedde. Terwijl veel organisaties nog steeds migreren naar externe en hybride werkomgevingen, ligt de nadruk dit jaar op hoe het bedreigingslandschap zich heeft aangepast en hoe deze trends een beveiligingsrisico vormen voor je organisatie van bestaande en nieuw ontwikkelde bedreigingen.

Elk jaar analyseert **Jamf Threat Labs** de bedreigingen voor apparaten die op de moderne werkplek worden gebruikt. Naarmate het personeelsbestand verder wordt verspreid, blijft onze kijk op het moderne bedreigingslandschap zich ontwikkelen om te voldoen aan de consistente vereisten van eindpuntcompliance, waarbij de beveiliging van gegevens wordt gewaarborgd terwijl de privacy van gebruikers wordt gehandhaafd in het licht van evoluerende risico's.

In het rapport van dit jaar worden vijf belangrijke beveiligingstrends onderzocht die van invloed zijn op organisaties, waarbij gebruikers op afstand verbinding maken met een veelheid aan apps en diensten die worden gehost in private en publieke datacenters en vertrouwen op verschillende cross-platform mobiele apparaten.

De trends van 2023 gaan over:

1. social engineering
2. gebruikersprivacy
3. nieuwe bedreigingen
4. compliance
5. verspreiding van het personeel

Trend 1 – Social engineering blijft de belangrijkste bedreiging

Social engineering, phishing-aanvallen in het bijzonder, staat bovenaan de lijst van belangrijke cyberbeveiligingsdreigingen. De vluchtige mix van een verspreid personeelsbestand met het relatieve gemak waarmee slechte actoren phishingcampagnes kunnen uitvoeren, leidt tot het succesvol verkrijgen van gebruikersgegevens. Deze aanvalstypen die ook wel 'de sleutels tot het koninkrijk' genoemd worden, verlenen onbevoegde gebruikers toegang tot gegevens die lokaal in het apparaat zijn opgeslagen. Wat deze aanvallen gevaarlijker (of impactvoller) maakt, is dat ze vaak toegang verlenen tot andere systemen als onderdeel van hun aanvalsketen.

De ironie van social engineering-aanvallen is dat ondanks sterke beveiligingsconfiguraties die voldoen aan de best practices in de sector, veel oplossingen weinig kunnen doen om dit soort aanvallen te voorkomen als gebruikers worden overgehaald om hun gegevens te overhandigen aan slechte actoren, die zich voordoen als iemand die ze niet zijn. Nog erger is hoe versnipperd omgevingen zijn geworden, waardoor veel gebruikers geen gemakkelijke toegang hebben tot IT- en beveiligingsprofessionals wanneer er verdachte e-mails of sms-berichten worden bezorgd die een onmiddellijke reactie lijken te vereisen.

Helaas is helaas zo dat het vanwege de opkomende aard van de berichten meestal te laat is tegen de tijd dat de gebruiker met IT heeft gesproken. De berichten zijn opzettelijk zo geschreven om slachtoffers af te schrikken zodat ze op een link klikken die hun authenticatietokens steelt, kwaadaardige code uitvoert om een kwetsbaarheid op hun apparaat te misbruiken of het slachtoffer gewoon naar een nepwebsite leidt die zich voordoet als een legitieme website en hen verleidt hun gegevens te verstrekken. **IBM meldde** bijvoorbeeld dat gestolen of gecompromitteerde gegevens niet alleen de meest voorkomende oorzaak van een datalek waren, maar dat het met 327 dagen ook het langst duurde om ze te identificeren.

Phishing-aanvallen verschillen nogal van andere soorten aanvallen: het zijn geen anonieme acteurs die liegen om je gebruikersnaam en wachtwoord te bemachtigen. Het bedrog kan op verschillende manieren worden uitgevoerd om hetzelfde resultaat te bereiken: neem bijvoorbeeld een populaire aanval die overal wordt uitgevoerd waar openbare hotspots (zie 'gratis wifi') beschikbaar zijn, genaamd 'evil twin'. Een evil twin doet zich voor als een legitiem draadloos netwerk, waardoor een aanvaller effectief alle relevante gegevens kan stelen die door het slachtoffer zonder zijn medeweten worden verzonden, wat kan worden voorkomen als het apparaat dat toegang heeft tot het netwerk is versleuteld met een **VPN of Zero Trust Network Access (ZTNA)-oplossing**.

In 2022 werd bij 31% van de organisaties ten minste één gebruiker het slachtoffer van een **phishing-aanval.**

In 2022 bleek 16% van de gebruikers gevoelige gegevens bloot te stellen door verbinding te maken met **riskante hotspots.**

Samen suggereren deze twee gegevenspunten dat:

1. gebruikers veel minder knoeien met hun apparaten dan vroeger, en...
2. slechte actoren hun aanvallen op bedrijfsapparaten opvoeren.

Bron: Jamf Threat Labs

Statistica schat dat er momenteel **wereldwijd 432,5 miljoen openbare wifi-hotspots beschikbaar** zijn**.** En in 2022 bleek 16% van de gebruikers gevoelige gegevens bloot te stellen door verbinding te maken met riskante hotspots. Ervan uitgaande dat slechts één gebruiker verbinding maakt met elke riskante hotspot, zou dat neerkomen op 432,5 miljoen gebruikers die gegevens doorgeven via niet-vertrouwde netwerkverbindingen.

De cijfers maken geen onderscheid tussen zakelijke en particuliere gebruikers, en houden evenmin rekening met oplossingen voor de beveiliging van eindpunten die kunnen helpen bij het verijdelen van phishing-aanvallen, zoals software voor het filteren van content die expliciet de toegang verhindert tot schadelijke URL's en domeinen die met phishing-campagnes in verband worden gebracht.

Het belangrijkste is dat ze volgens de EC-Council geen rekening houden met **de beste manier om je personeel te beveiligen.** Of het nu gaat om het bestrijden van social engineering-bedreigingen of het afslaan van phishing-aanvallen via allerlei communicatiemiddelen, een van de beste verdedigingsmaatregelen is geen beveiligingscontrole maar een administratieve controle, namelijk **cyberbewustzijnstraining.** Met een uitgebreid trainingsprogramma voor gebruikers dat is ingebouwd in je onboardingprocessen en regelmatige updates die zijn toegespitst op de aanvallen die talloze organisaties wereldwijd treffen, voelen gebruikers zich gesterkt in hun kennis om bedreigingen te herkennen en de risico's in te schatten die gepaard gaan met het opvolgen van phishingpogingen.

Investeren in beveiligingsbewustzijnstrainingen voor belanghebbenden is een belangrijk onderdeel van de beveiligingsstrategie van een bedrijf en mag niet over het hoofd worden gezien. Dit betekent de implementatie van voortdurende, veelzijdige training voor eindgebruikers die een verscheidenheid aan best practices omvat en gebruikers voorlicht over de nieuwste bedreigingen die hen het meest waarschijnlijk zullen treffen. Hierdoor kunnen zij nieuwe en zich ontwikkelende aanvallen identificeren en proactief stappen ondernemen om hun veiligheidshygiëne te verbeteren, zowel op het werk als in hun privéleven.

De top 10 van soorten phishing-aanvallen zijn:

1 **E-mail:**
E-mailberichten worden verstuurd naar personen die doen alsof ze afkomstig zijn van een gerenommeerde, betrouwbare bron.

2. **Vishing:**
Voice phishing-aanvallen schakelen over op een op de telefoon gerichte aanval (TOAD), waarbij vaak het nummer van de beller wordt 'gespooft' om zich voor te doen als een betrouwbare bron. Zoals de zwendelgesprekken die beweren van de FBI te zijn.

3. **Smishing:**
Net als bij Vishing gebruiken bedreigers sms-berichten met links of bijlagen in plaats van telefoongesprekken om gebruikers van mobiele apparaten te compromitteren.

4. **Social Media/Angler:**
Nieuwe technologie leidt tot nieuwe aanvalsvectoren, vandaar dat deze aanvallen gericht zijn op gebruikers van social media op verschillende platforms. De laatste, Angler phishing, is een nieuwere variant op het thema social media, waarbij aanvallers zich voordoen als klantenservicemedewerkers, vaak compleet met een nepprofielaccount, om zich te richten op slachtoffers die hulp nodig hebben.

5. **Spear:**
Een variant van e-mail phishing die gebruik maakt van een gerichte aanpak, gericht op specifieke personen binnen een organisatie, zoals een werknemer van de salarisadministratie.

6. **Whaling:**
Vergelijkbaar met spear phishing, maar deze aanval verfijnt het bereik tot leidinggevenden en directieleden.

7. **HTTP/S:**
Op websites gebaseerde aanvallen waarbij URL's worden gebruikt die vaak subtiele spelfouten bevatten die moeilijk in één oogopslag te herkennen zijn, zoals "iamf.com" in plaats van jamf.com. Het kan ook gaan om SSL-beveiligde domeinen die legitiem zijn geregistreerd om de beveiligingscontrolefuncties van moderne browsers te omzeilen.

8. **Websitevervalsing:**
Dit aanvalstype gaat vaak gepaard met HTTP/S-aanvallen, waarbij een legitiem ogende website wordt gekoppeld aan de kwaadaardige URL, compleet met de originele tekst, logo's, kleurenschema's en functionaliteit die de eigenlijke website weerspiegelt, zodat deze er betrouwbaar uitziet.

9. **Watering hole:**
Deels spear phishing, deels tactisch, zijn watering hole-aanvallen gericht op specifieke groepen gebruikers en een website die zij vaak bezoeken. De aanval is erop gericht de website te compromitteren en met malware te besmetten, zodat wanneer de beoogde gebruikers de site bezoeken, ook zij besmet raken.

10. **Pop-up:**
Net als de pop-up-advertenties van de technologie van weleer, vereist deze variant op phishing dat slechte actoren een website infecteren met malware, vervolgens gebruikmaken van ingesloten advertenties of nieuwere meldingen die door gebruikers zijn ingeschakeld en gebruikers infecteren wanneer de payload wordt afgeleverd.

Trend 2 – De privacy van de gebruiker krijgt een plaats aan de beveiligingstafel

Terwijl fabrikanten en ontwikkelaars, zoals Apple en Jamf, al enige tijd geleden de handen ineengeslagen hebben op het gebied van privacy, hebben andere technologieleveranciers over het algemeen in het verleden niet evenveel aandacht besteed aan privacybescherming als aan andere beveiligingsmaatregelen in hun hardware- en softwareaanbod.

Net als de gevolgen van het uitlekken van persoonlijke en zakelijke gegevens, maakt het slagveld over de bescherming van privacygegevens van gebruikers veel slachtoffers als het wordt geschonden. Bedenk dat persoonsgegevens niet zomaar zonder toestemming van de gebruiker worden verzameld. Het wordt op verschillende manieren gecompromitteerd:

- Nationale staten gebruiken kwaadaardige code waarmee communicatiemiddelen, zoals de cameramicrofoon of key-logging op apparaten van slachtoffers, kunnen worden afgeluisterd om hen te bespioneren.
- Kwaadwillenden gebruiken deze gegevens voor persoonlijk of financieel gewin, maar ook om social engineering-campagnes uit te breiden en slachtoffers te chanteren.
- Bedrijven verrijken zich door verzamelde gegevens zonder toestemming van de gebruiker te verkopen aan adverteerders en/of derde partners.

In andere gevallen komen organisaties die persoonsgegevens verzamelen als onderdeel van hun legitieme operationele procedures in de problemen door onvoldoende bescherming van persoonsgegevens tegen een externe aanval, een bedreiging van binnenuit of regelgevende governance. En in sommige gevallen **zijn organisaties zich niet eens bewust van de bedreiging**, zoals blijkt uit het feit dat '5% van de organisaties in 2022 een potentieel ongewenste toepassing heeft geïnstalleerd in hun apparatenvloot.'

Op het eerste gezicht lijkt 5% niet significant. Maar risicobeoordeling gaat veel verder dan alleen cijfers. Het houdt rekening met het volgende:

- identificatie van gerichte assets
- alle aanwezige aanvalsvectoren
- soorten mogelijke aanvallen
- waarschijnlijkheid van een aanval
- potentiële impact indien uitgebuit of gecompromitteerd

In wezen stelt de combinatie ervan organisaties in staat te beoordelen welk risico aanwezig is en hoe dit de bedrijfscontinuïteit zal beïnvloeden. Hoe geldt dit voor persoonsgegevens?

'**0,4%** van de Android-apparaten was in **2022** een potentieel ongewenste app geïnstalleerd, tegenover **0,1%** van de iOS-apparaten.'

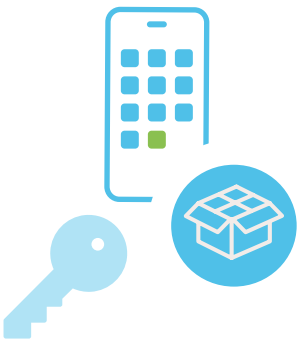
Android is een open ecosysteem dat leidt tot meer risicovolle apps. Apple heeft een gecureerd app-ecosysteem gecreëerd en biedt de gebruiker strengere privacybescherming die de introductie van deze risicovolle apps beperkt.

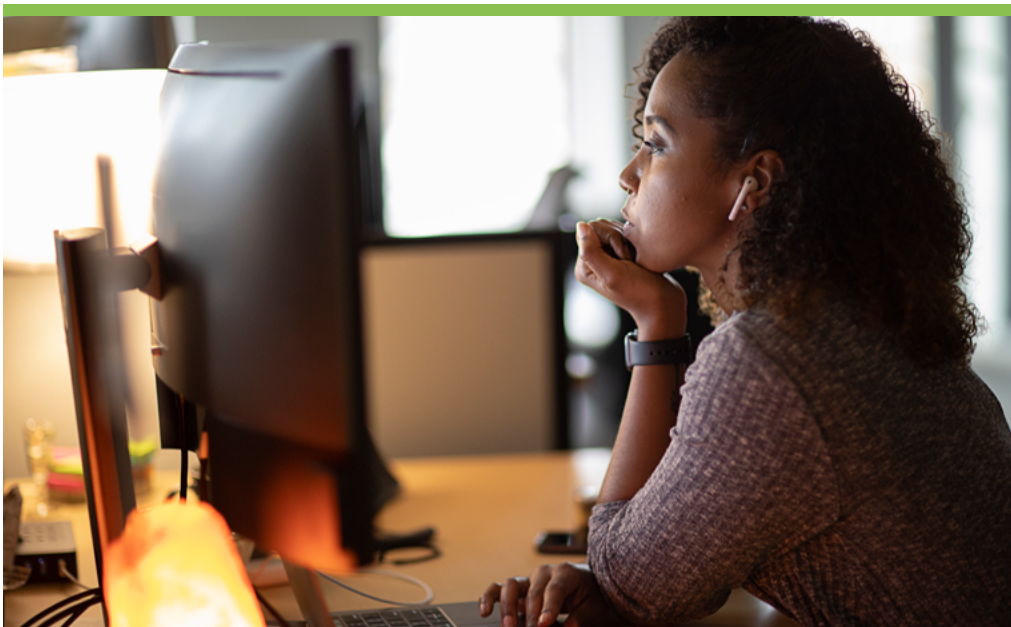
Het laatste punt betreffende de potentiële impact bij misbruik of compromittering kan niet worden onderschat, omdat het rechtstreeks de kern raakt van regelgevingscontroles en hoe deze werken om risico's te beperken. Zij voorkomen namelijk datalekken die in strijd zijn met de regelgevingswetgeving (meer over compliance verderop in dit rapport).

Effectieve privacycontroles worden steeds belangrijker naast beveiligingscontroles — niet alleen om waar nodig compliance af te dwingen, maar ook om de blootstelling van privacygegevens van gebruikers te beperken als onderdeel van de grotere beveiligingsstrategie. Het moet zich uitstrekken tot alle oplossingen, processen, belanghebbenden en workflows binnen een organisatie om de algemene gegevensbeveiliging op te bouwen naast het creëren of implementeren van alle componenten in de onderneming. Het mag niet slechts een bijzaak zijn.

Beheeroplossingen helpen het beleid van de organisatie af te stemmen op de eisen van de regelgeving en verlichten de beheerlast door IT in staat te stellen bedrijfsapps aan te wijzen. Dit zorgt ervoor dat alle soorten gegevens in de hele infrastructuur worden beveiligd, ongeacht het type apparaat of de locatie.

Door gebruik te maken van het beheer van meerdere eigendomsmodellen voor apparaten vinden organisaties een evenwicht tussen het beveiligen van apps en gegevens en het toepassen van veilige configuraties op de apparaten zelf om veilig toegang te krijgen tot bedrijfsmiddelen. Tegelijkertijd kunnen gebruikers uiteindelijk de privégegevens in verband met hun persoonlijke apps en apparaatgebruik controleren. Bedrijven beschermen bedrijfseigen gegevens die zowel gevoelig als vertrouwelijk zijn en handhaven tegelijkertijd een 'hands-off' benadering van privégebruikersgegevens, **waardoor eindgebruikers het niveau van toegang** tot deze gegevens kunnen bepalen. Hierdoor wordt de algehele privacybescherming verder verbeterd, ongeacht of apparaten deel uitmaken van een BYOD-programma, apparaten van het bedrijf die deel uitmaken van een CYOD/COPE-initiatief of een mix van deze modellen.





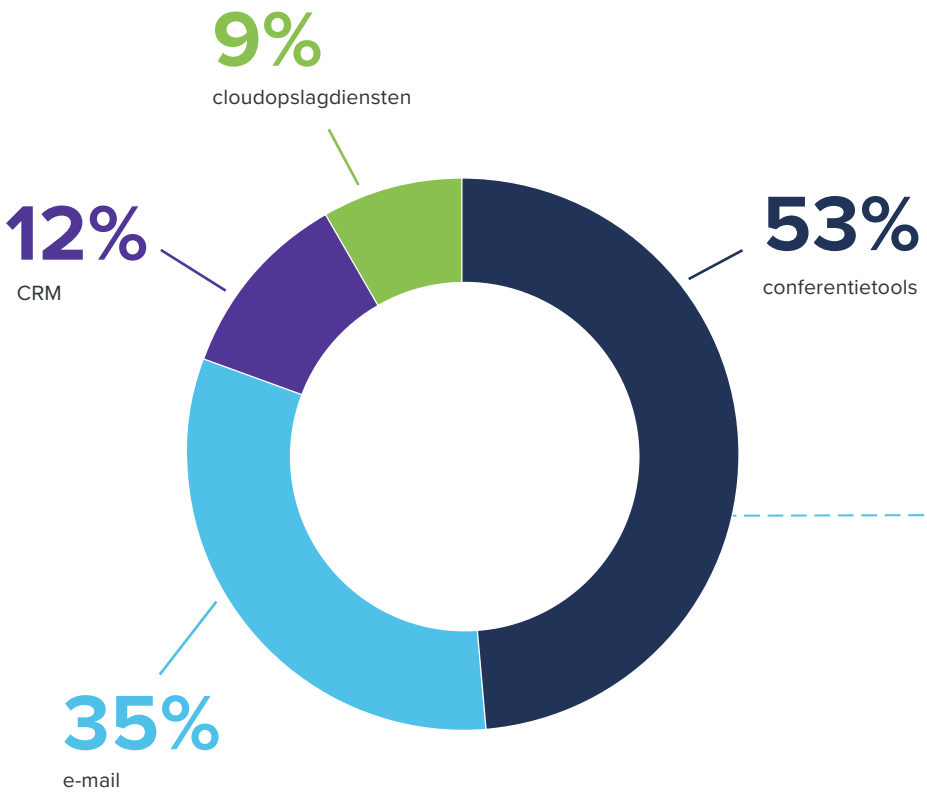
Trend 3 – Slechte actoren voegen aanvallen samen tot nieuwe bedreigingen

Goed nieuws op het gebied van macOS-malware: het totale aantal malware-infecties vertoonde geen tekenen van groei ten opzichte van het voorgaande jaar. Het betere nieuws – in 2022 **daalden de nieuwe malware-infecties** van iets meer dan 150 miljoen naar ongeveer 100 miljoen infecties, volgens AV-Atlas' voortdurende registratie van schadelijke programma's en potentieel ongewenste toepassingen (PUA).

Kwaadaardig netwerkverkeer, dat verwijst naar netwerkgebaseerde Indicators of Compromise (IoC's) die kunnen worden waargenomen in de communicatiepatronen tussen het apparaat en internetservers, komt steeds vaker voor. Kwaadaardig netwerkverkeer wordt meestal alleen waargenomen in productieomgevingen en kan niet worden geïdentificeerd door eenvoudigweg statische code te beoordelen. Daarom is actieve controle van de gezondheid van de eindpunten zo cruciaal bij de beoordeling van gecombineerde risicofactoren.

Het is op zich niet nieuw dat kwaadwillenden verschillende aanvallen combineren, maar in het moderne bedreigingslandschap worden meer van deze samengevoegde bedreigingen actief in het wild gebruikt om werknemers die verspreid zijn op nieuwe manieren aan te vallen en ongeoorloofde toegang te krijgen tot beschermde diensten en middelen. In één maand van 2022 had 53% van de gecompromitteerde apparaten toegang tot conferentiemiddelen, terwijl 35% toegang had tot e-mail, 12% tot een CRM en 9% tot cloudopslagdiensten.

In één maand van 2022 had **53%** van de gecompromitteerde apparaten toegang tot conferentiemiddelen, terwijl **35% toegang had tot e-mail**, **12% tot een CRM** en **9% tot cloudopslagdiensten.**



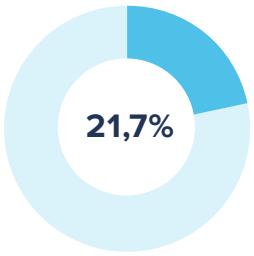
Geavanceerd aanvalsvoorbeeld

Een werknemer ontvangt een spear phishing-bericht dat van een collega lijkt te komen. Het bericht bevat een link naar een 'werkdocument', dat kwaadaardige code op het apparaat van het slachtoffer injecteert die hun referenties verzamelt en tevens een ransomware payload levert. Terwijl hij de gevoelige gegevens overneemt, gebruikt de aanvaller de gegevens om meer toegang te krijgen tot de infrastructuur van de organisatie. Ten slotte vervult de kwaadwillende nog twee functies: hij voegt het eindpunt toe als onderdeel van een botnet dat wordt gebruikt om andere organisaties aan te vallen en zoekt andere apparaten om te infecteren, waardoor het proces wordt uitgebreid en het botnet groeit.

De overkoepelende boodschap hier is dat aanvallen meer dan één vorm kunnen aannemen en over elke periode kunnen plaatsvinden en vaak onopgemerkt blijven. Sommige aanvalsketens treden kort na de compromittering op, zoals ransomware, terwijl andere tactischer zijn en meer tijd vergen, zoals het bouwen van een botnet om systemen aan te vallen met DDoS-aanvallen (denial of distributed service).

Deze convergentie is moeilijk te bestrijden omdat de slachtoffers meestal de omvang van de aanval niet kennen tot de volgende golf hen begint te treffen. Toch kunnen bepaalde praktijken sommige risico's beperken en de gevolgen van andere ernstig beperken of verzachten. Het actief bewaken van eindpunten en het verzamelen van telemetriegegevens over de gezondheidsstatus van eindpunten is een essentiële gegevensbron voor beheerders, omdat het diepgaand inzicht biedt in apparaten en hoe zij ervoor staan met betrekking tot verschillende vectoren, zoals patchniveaus, vooral omdat verdacht gedrag dat erop kan wijzen dat een apparaat gecompromitteerd is, niet wordt gezien of gevoeld door een eindgebruiker.

Over patchbeheer gesproken, het beheer van de levenscyclus van apps is van essentieel belang om het risico van systeemkwetsbaarheden te beperken en er tegelijkertijd voor te zorgen dat apps zo goed mogelijk beveiligd zijn tegen bekende bedreigingen. Dit is vooral belangrijk als je bedenkt dat app-winkels van derden vaak versies van legitieme apps aanbieden die kwaadaardige code bevatten, waardoor apparaten van gebruikers worden geïnfecteerd. Denk bijvoorbeeld aan de gratis versies van betaalde apps als lokaas om slachtoffers te lokken.



21,7% van de Android-apparaten had toegang tot app stores van derden, vergeleken met **0,002%** van de **iOS-apparaten.**

App stores van derden zijn een gebruikelijke manier om het beoordelingsproces van apps, dat apparaten en gebruikers beschermt, te ondermijnen.

0,02% van de Android-apparaten was geroot en **0,001%** van de **iOS-apparaten** was **jailbroken** in 2022.

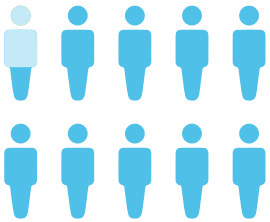
Ondanks het kleine percentage is het opvallend dat het aantal getroffen Android-apparaten twee keer zo groot is als dat van Apple. En als je denkt aan de abstracte hoeveelheid Android- en Apple-apparaten in de wereld, is de omvang hiervan niet moeilijk voor te stellen.

Hoewel bepaalde besturingssystemen (OS) het side-loaden van toepassingen toestaan, vereisen andere, zoals iOS, dat apparaten eerst worden gejailbreakt om de bescherming te omzeilen die iOS-gebaseerde apparaten beschermt tegen het uitvoeren van niet-ondertekende code. Het vergrendelen van apparaten is slechts een deel van de oplossing. Het is van cruciaal belang jailbroken apparaten in realtime te identificeren om deze bedreigingsvector doeltreffend aan te pakken.

Aanvallen op de toeleveringsketen

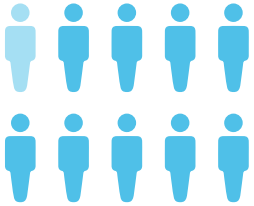
Aanvallen tegen de toeleveringsketen of **derden** hebben historisch gezien een bredere impact die verschillende lagen diep gaat in - en door organisaties in de pijplijn – alvorens het eigenlijke doelwit van de **aanvaller te bereiken.** De gevolgen zijn vaak verstrekkend en treffen bedrijven wereldwijd, ongeacht de sterkte van hun beveiliging.

Het voorkomen van deze aanvallen is een heikel punt, vooral omdat organisaties niet de bevoegdheid hebben om van elke organisatie (of hun contractanten) in de pijplijn te eisen dat zij de risicofactoren op zinvolle wijze beperken. Helaas geldt om dezelfde redenen hetzelfde voor de bescherming van je organisatie tegen deze bedreigingen. Maar zoals het Cybersecurity and Infrastructure Security Agency (CISA) en het National Institute of Standards and Technology (NIST) in hun gezamenlijke technische document **Defending Against Software Supply Chain Attacks** aangeven, is een belangrijk element om 'het vermogen van een organisatie om dergelijke aanvallen te voorkomen, te beperken en erop te reageren' te versterken, de compliance van de beste praktijken in de sector als onderdeel van een alomvattende defense-in-depth beveiligingsstrategie. Dit omvat het doorlichten van de beveiligingsprocessen van leveranciers door onafhankelijke auditors van derden om na te gaan of je partners (en vervolgens hun partners) de juiste risicobeperkende maatregelen nemen voordat een aanval heeft plaatsgevonden.



0,004% van de gebruikers en **0,3%** van de organisaties had in 2022 een **jailbroken** of **geroot** apparaat.

Statistieken van vorig jaar:



Minder dan 1% van de organisaties had in 2021 een **jailbroken** of **geroot** apparaat.

Trend 4 – Voldoen aan regelgeving maakt deel uit van de security stack

Een groeiende trend, naast de beveiliging van organisatorische gegevens, is het belang van de privacy van de gebruiker. Dit komt het meest voor bij compliance, met name van Europese en nationale voorschriften. Bedenk hoe de Algemene verordening gegevensbescherming (AVG) het recht van gebruikers op privacy op nationaal beter beschermen of hoe fintech – een van de meest gereguleerde sectoren wereldwijd – aan meerdere facetten van governance is onderworpen.

Hier volgen enkele voorbeelden van hoe meerdere regelgevingswetten in de VS op zichzelf of in combinatie met elkaar werken om in bepaalde bedrijfstakken aan de regelgeving te voldoen:

Sarbanes-Oxley Act van 2002 (SOX): dicteert specifieke voorwaarden voor boekhoudpraktijken

Gramm-Leach-Bliley Act (GLB): met betrekking tot de minimumniveaus van cyberbeveiliging die vereist zijn om de informatiebeveiliging in stand te houden

Financial Industry Regulatory Authority (FINRA): geeft expliciet aan hoe bedrijfsprocessen verband houden met het waarborgen van de bescherming van beleggers door middel van eerlijke en oprechte transacties binnen de effectenindustrie.

In het licht van de compliance-voorschriften die van invloed zijn op bedrijven in bepaalde sectoren en hun wereldwijde bereik, waardoor betrokken organisaties moeten voldoen aan wetten die ver buiten hun jurisdictie kunnen liggen, moeten organisaties meer controle uitoefenen over workflows. Dit is nodig voor de handhaving van de privacy en het beheer van beschermde gegevenstypen, zoals persoonlijk identificeerbare informatie (PII), beschermde gezondheidsinformatie (PHI) en business intelligence-informatie (BII) , terwijl deze worden verzameld, verwerkt, opgeslagen, gewijzigd, gedeeld en vernietigd volgens de wensen van de gebruiker en/of voorschriften.

Compliance kan een moeilijke taak zijn die serieuze aandacht, beheer en ondersteuning vereist, zelfs als je apparaten en gegevens door de organisatie worden beheerd. Maar hoe zit het met het afdwingen van compliance door een verspreid personeelsbestand dat overal, op elk apparaat en op elk moment toegang moet kunnen krijgen tot bedrijfsmiddelen? De extra complicaties van personeel dat op afstand, hybride of op locatie werkt kunnen een pijnpunt vormen voor organisaties die aan compliance-eisen moeten voldoen en die door het moderne bedreigingslandschap navigeren.

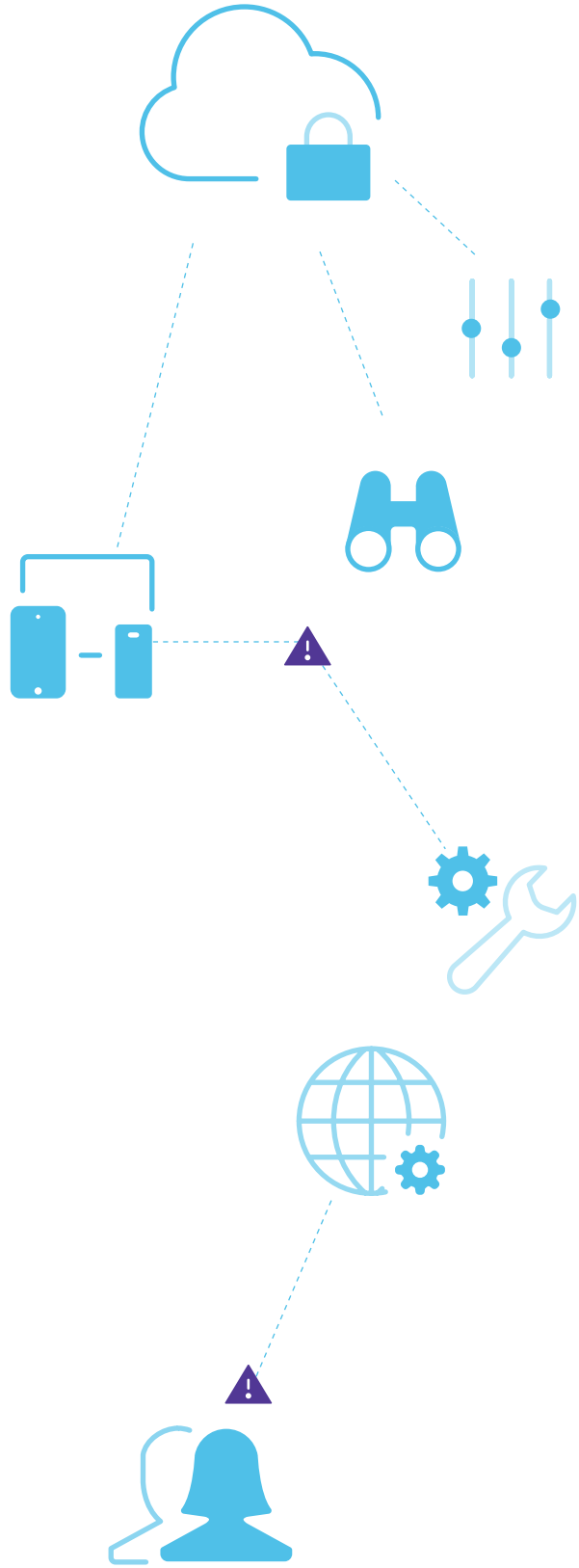
In **2022** gebruikte **21%** van de werknemers apparaten die verkeerd **geconfigureerd** waren, waardoor ze **risico's** liepen.

Helaas wordt het compliancewater alleen maar troebeler wanneer ook persoonlijke apparaten in de mix worden opgenomen. In 2022 gebruikte 21% van de werknemers apparaten die verkeerd geconfigureerd waren, waardoor ze risico's liepen. Sterker nog, gegevens die gevoelig, vertrouwelijk of missiekritisch kunnen zijn – en mogelijk gereglementeerd – lopen het risico te worden blootgesteld, waardoor de organisatie (en mogelijk ook de gebruiker) civielrechtelijk en/of strafrechtelijk aansprakelijk wordt gesteld als daardoor overtredingen van de regelgeving worden vastgesteld.

Hoewel veel organisaties een vorm van BYOD of een keuzeprogramma voor werknemers hebben ingevoerd, waarbij eindgebruikers kunnen kiezen welke soorten apparaten en besturingssystemen zij het meest productief en comfortabel vinden, kan de oplossing voor effectief compliancebeheer niet alleen bestaan uit het uitsluiten van alle apparaten, behalve de beheerde. **We zagen dat 8% van de gebruikers en 21% van de organisaties getroffen werden door kwetsbaarheden in de configuratie**, wat betekent dat zelfs apparaten die eigendom zijn van het bedrijf en beheerd worden, getroffen kunnen worden. Oplossingen moeten meer rekening houden met beveiligingsproblemen dan alleen apparaatbeheer.

Het is namelijk denkbaar dat elk eindpunt op elk moment een patch mist, gegevens lekt als gevolg van een kwetsbaarheid in de koppeling of gewoon verloren of gestolen wordt. In elk scenario zou een andere actie nodig zijn om het risico te beperken. Sommige situaties kunnen worden aangepakt via geautomatiseerde respons- en herstelworkflows, maar het punt blijft dat er ook altijd een plaats zal zijn voor handmatig herstel.

Zoals bij de meeste discussies over beveiliging zijn er geen kant-en-klare oplossingen die alle aspecten dekken die nodig zijn om je infrastructuur altijd compliant te houden. Wij adviseren een defense-in-depth beveiligingsstrategie te implementeren die meerdere convergerende oplossingen biedt om je unieke compliance-eisen vanuit vele invalshoeken aan te pakken.



Trend 5 – Beveiliging van gegevens in externe/hybride omgevingen vormt nog steeds een uitdaging

De verschuiving naar werknemers op afstand bracht veranderingen met zich mee voor de beveiliging van gebruikers, gegevens en apparaten. Nu de netwerkperimeter effectief is uitgehold, zijn on-premise oplossingen vervangen door cloud-gebaseerde oplossingen om beveiligingsdiensten te distribueren naar gebruikers die op elk apparaat vanaf elke locatie werken. Het resultaat was een eindpuntbeveiligingsoplossing die beter in staat en zelfvoorzienend was, met toegevoegde veerkracht en sterke applicatiebeveiliging.

En toch, ondanks de vastgestelde voordelen, ondervinden organisaties enkele jaren na de migratie nog steeds problemen met de gegevensbeveiliging van externe en hybride werkomgevingen. Helaas kan er geen duidelijke boosdoener worden aangewezen. Een combinatie van problemen draagt ertoe bij dat gegevens onvoldoende worden beveiligd. Sommige van deze problemen komen voort uit een gebrek aan:

- realtime inzicht in de gezondheid van eindpunten
- integratie tussen beheers- en beveiligingstooling
- geautomatiseerde processen en workflows
- gedecentraliseerde registratie en informatie over bedreigingen
- handhaving van beleid en compliance
- veiligheidstrainingsprogramma's voor eindgebruikers
- best-of-breed oplossingen
- risicobeoordelingspraktijken om activa en bedreigingen te identificeren

Zo bleek dat **64% van de kwetsbare apparaten toegang had tot samenwerkingstools en 34% tot e-mail van de onderneming.** Dit geeft aan dat, hoewel risico- en compromisindicatoren subjectief zijn en van bedrijf tot bedrijf zullen verschillen, routinetaken zoals patchbeheer niet op alle apparaten plaatsvinden. Hierdoor lopen de apparaten zelf gevaar en lopen ook de middelen van de organisatie gevaar. Het gaat zelfs verder dan apps en configuraties. Jamf Threat Labs ontdekte dat **1 op de 5 apparaten een besturingssysteem had dat niet up-to-date was.** Het is essentieel dat er beveiliging bestaat op alle lagen van een defense-in-depth strategie, te beginnen op besturingssysteemniveau, voor de bescherming van gebruikers en organisaties.

Dit onderstreept nog eens de reële behoefte aan inzicht in je apparatenvloot en de interactie daarvan met de infrastructuur van je organisatie, vooral als je sector gereglementeerd is. Deze vereiste wordt nog versterkt wanneer je bedenkt dat de meeste regelgevende instanties eisen dat organisaties hun compliance aantonen door middel van regelmatig geplande audits die worden uitgevoerd door regelgevende instanties die willen controleren of de beschermde gegevens en de eindpunten die ermee interageren beveiligd zijn in overeenstemming met de regelgevende governance.

Maar het beoordelen van de middelen en bedreigingen die van invloed zijn op je organisatie en de bijbehorende telemetrie om getroffen eindpunten te identificeren is slechts een deel van de oplossing. Er zijn moderne oplossingen nodig om risico's te beperken en realtime-toegangsbeslissingen af te dwingen. Oudere technologieën, zoals VPN voor het beveiligen van verbindingen op afstand, kunnen zeker niet concurreren met nieuwere technologieën die zijn ontworpen om de uitdagingen van verspreide werkplekken en het moderne bedreigingslandschap aan te pakken. ZTNA staat verbindingen met apps en diensten alleen toe nadat is geverifieerd dat het apparaat en de gebruiker toegang hebben tot de gevraagde diensten en voldoen aan de minimale 'gezondheids'-vereisten om dit veilig en beveiligd te doen.

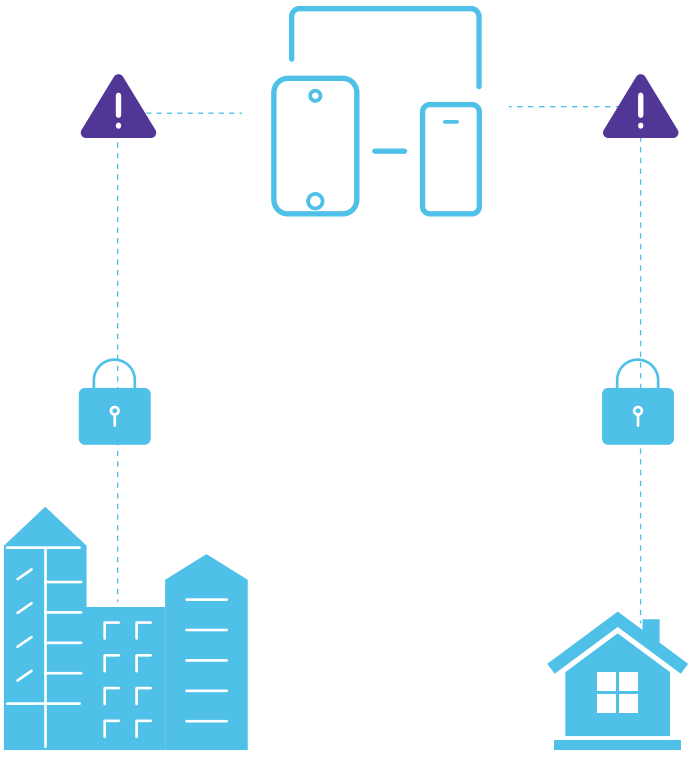
De oplossingen van ZTNA zijn ontworpen met moderne netwerken en workflows in gedachten en beperken de risico's en beschermen gegevens terwijl ze flexibel genoeg zijn om ervoor te zorgen dat persoonlijke apps en gegevens privé blijven. Daarnaast hebben geautoriseerde gebruikers alleen toegang tot de apps waartoe zij toegang hebben volgens het beginsel dat alleen strikt noodzakelijke rechten worden toegekend, terwijl het zakelijke verkeer door microtunnels wordt geleid, wat voorkomt dat aanvallers die een enkele gebruiker compromitteren, toegang krijgen tot alle applicaties waartoe de gebruiker toegang heeft. Door ingebouwde segmentatie van verkeerstunnels wordt voorkomen dat aanvallers laterale bewegingen door het netwerk uitvoeren, waardoor bedreigingen effectief worden beperkt.

Een ander belangrijk onderdeel is de veilige integratie van oplossingen door gebruik te maken van API's om kritieke telemetrie- en eindpuntgezondheidsgegevens te delen met oplossingen die de slagingskans van bedreigingen voor apparaten, gebruikers en gevoelige gegevens beperken. Dit staat in schril contrast met 'bolt-on' of op zichzelf staande oplossingen, waarbij off-the-shelf beveiligingstools onafhankelijk werken, maar de integratiecomponent ontbreekt die een holistische, defense-in-depth oplossing aandrijft.

Naarmate kwaadwillenden hun tools ontwikkelen, moeten organisaties hun oplossingen gebruiken om bekende aanvallen te voorkomen en het risico van nieuwe aanvallen te beperken. Met dat laatste in gedachten blijft threat hunting (het proactief onderzoeken van bedreigingen die mogelijk je beveiligingscontroles hebben omzeild en nog niet zijn gedetecteerd) groeien en bloeien binnen organisaties, door hun IT- en beveiligingsteams te helpen bij het identificeren, beperken en verhelpen van onbekende en nieuwe bedreigingen voordat deze kunnen leiden tot inbreuken op gegevens. Artificial Intelligence (AI) en Machine Learning (ML) hebben hun doeltreffendheid bewezen in verschillende sectoren, en cyberbeveiliging is er een van, omdat oplossingen steeds meer gebruikmaken van de uitgebreide verwerkingskracht en mogelijkheden voor gedragsanalyse om actoren van bedreigingen en hun aanvallen te leren, efficiënt te voorspellen en tegen te gaan met een snelheid waarmee menselijke beheerders eenvoudigweg niet kunnen concurreren.

Richt je strategie op het beheer van mobiele apparaten (MDM) om zowel persoonlijke als bedrijfsapparaten te beveiligen en patches up-to-date te houden. Zet eindpuntbeveiliging in om malware te voorkomen en verzamel tegelijkertijd rijke telemetriegegevens door actieve bewaking van eindpunten. Een API is een uitstekende manier om gegevens over bedreigingen veilig te delen tussen deze twee oplossingen en stelt organisaties in staat de compliance-eisen te handhaven door middel van op beleidsregels gebaseerde handhaving. Door oplossingen voor identiteits- en toegangsbeheer toe te voegen, worden het beheer van referenties en de verlening van machtigingen voor goedgekeurde organisatorische middelen gecentraliseerd en wordt multifactorauthenticatie (MFA) toegevoegd om de toegang te beveiligen.

Dit integreert met moderne beveiligingsoplossingen, zoals ZTNA, om verbindingen over elk netwerk te beveiligen, ML te integreren om op nieuwe bedreigingen te jagen, aanvallen te stoppen voordat ze kunnen beginnen en verouderde VPN's te vervangen door moderne oplossingen die toegangsverzoeken segmenteren om netwerkgebaseerde bedreigingen tegen te gaan. En uiteindelijk alle relevante bedreigingen en de gezondheidsstatus van het apparaat in realtime verzamelen om het levenscyclusbeheer van het apparaat holistisch te automatiseren.



Aanbevelingen

Nu het drie jaar geleden is dat de wereldwijde pandemie leidde tot een drastische verandering in wereldwijde werkomgevingen, is de aandacht voor velen verschoven van **'hoe kunnen we de bedrijfsvoering voortzetten?'** naar **'hoe kunnen we externe gebruikers en organisatorische middelen voortdurend beschermen?** '

Een van de belangrijkste redenen voor de mentaliteitsverandering is dat IT- en beveiligingsteams, ondanks het feit dat ze al enkele jaren op afstand werken, tegenwoordig meer dan het dubbele aantal externe gebruikers ondersteunen (46%) dan vóór de pandemie (21%), volgens het **rapport The State of Security 2022** van Splunk. Uit het wereldwijde onderzoek van Splunk blijkt dat 'we niet alleen meer aanvallen blijven zien, maar ook meer daadwerkelijke inbreuken'.

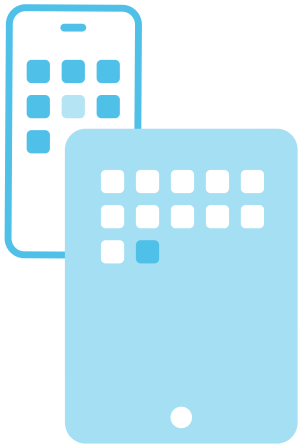
Deze combinatie van stijgende aanvalscijfers, een evoluerend bedreigingslandschap en een groeiende behoefte om middelen te beveiligen waartoe externe gebruikers toegang hebben, onderstreept de verklaring in het rapport Beveiliging 360 van vorig jaar:

> Beveiligde oplossingen voor toegang op afstand moeten flexibel en wendbaar genoeg zijn om productiviteit mogelijk te maken, niet te blokkeren en niet in de weg te zitten.

Dit jaar voegen we daaraan toe:

> Eindpuntbeveiliging moet convergentie van beveiligingsoplossingen bieden, waarbij een sterke basis en granulaire zichtbaarheid met geavanceerde technologieën, zoals ML, worden gebruikt om geautomatiseerde veilige workflows te ontwikkelen die in overeenstemming zijn met het beleid van de organisatie en de voorschriften van de sector.

uiteindelijk moeten organisaties een moderne, cloud-gebaseerde defense-in-depth beveiligingsstrategie ontwikkelen om in hun unieke behoeften van vandaag te voorzien en tegelijkertijd de schaalbaarheid te bieden om in de behoeften van morgen te voorzien.



Over dit onderzoek

Wij willen de grootste veiligheidstrends in de nieuwe wereld van hybride werken in kaart brengen. De informatie en statistieken in dit document zijn de resultaten van onze analyse van beveiligingstrends binnen een steekproef van 500.000 door Jamf beschermde apparaten, verspreid over iOS, macOS, iPadOS, Android en Windows, in 90 landen, over een periode van 12 maanden. Deze analyse werd uitgevoerd in het vierde kwartaal van 2022. De in dit onderzoek geanalyseerde metadata zijn afkomstig van geaggregeerde logbestanden die geen persoons- of organisatiegebonden informatie bevatten. Met deze analyse willen wij geen angst aanjagen, maar jou en je gebruikers informeren over de beschikbare opties en de beste manier om alle aspecten van apparaat-, gebruikers- en organisatiegegevens te beveiligen.