Wat is confidential computing en hoe werkt het?

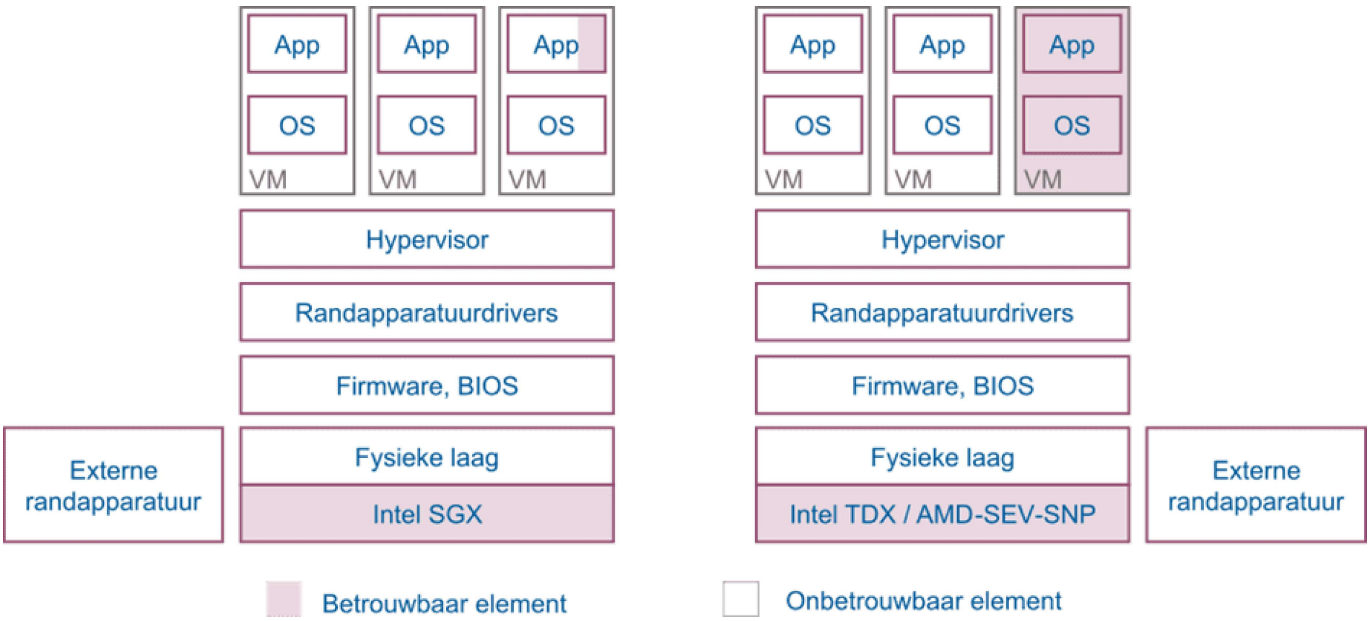
.devops 21.08.'23 10:00 21 min **Smals Research**

Confidential computing belooft gevoelige data beter te beschermen. AMD en Intel hebben hun eigen implementaties en ook AWS heeft een unieke oplossing. Hoe werken die oplossingen, en wat zijn de voor- en nadelen?

Om te voldoen aan de eisen van hun klanten die met gevoelige gegevens omgaan, of om nieuwe klanten aan te trekken, verrichten leveranciers van publieke IT-infrastructuren inspanningen om hun beveiliging te verbeteren en met name om de gegevens van hun klanten beter te beschermen. Microsoft, bijvoorbeeld, zegt elk jaar ongeveer een miljard dollar te investeren in de beveiliging van zijn infrastructuren. Sinds halfweg 2010 investeren deze infrastructuurleveranciers in een aanbod van *confidential computing*. Voornamelijk gebaseerd op *Trusted Execution Environments* (TEE), vermindert dit in principe het vereiste vertrouwen van de klant in de infrastructuurleverancier.

In dit artikel gaan we dieper in op hoe de belangrijkste commerciële implementaties werken. Het is echter belangrijk om in gedachten te houden dat de definities van *confidential computing* en TEE verschillen en soms onvolledig zijn. Dit kan leiden tot een vals gevoel van veiligheid, juridische onzekerheden en maakt het vergelijken moeilijk. Als reactie op dit gebrek aan standaardisatie en interoperabiliteit tussen de verschillende benaderingen van *confidential computing* is het *Confidential Computing Consortium* opgericht door grote spelers in de sector, waaronder AMD, Google, Intel en Microsoft. Daarbij moeten we opmerken dat Amazon geen deel uitmaakt van dit consortium en dat zijn Nitro-systeem sterk afwijkt van de andere benaderingen.

de *confidential computing* in grote data centers. Terwijl Intels TDX en AMD's SEV-SNP-technologieën ontwikkeld zijn om complete *virtual machines* (VM's) te beschermen, is de SGX-technologie erg verschillend en heeft deze een kleiner *attack surface*. Figuur 1 toont de elementen die de *Trusted Computing Base* (TCB) vormen voor deze drie technologieën die we in de volgende paragrafen beschrijven.



Figuur 1 – Intels SGX-technologie kan worden gebruikt om een proces te isoleren, terwijl Intels TDX- en AMD's SEV-SNP-technologieën kunnen worden gebruikt om hele virtuele machines te isoleren.

AMD's SEV-SNP-technologie

In 2016 introduceerde AMD de technologie *Secure Encrypted Virtualisation* (SEV) om VM's op hardwareniveau te isoleren van de hypervisor. Elke VM ontvangt zijn eigen AES-coderingssleutel voor geheugenversleuteling. De status van de microprocessorregisters van elke VM wordt ook versleuteld, waardoor de hypervisor de gegevens in de VM niet kan lezen.

Later voegde AMD de technologie *Secure Nested Paging* (SNP) toe om geheugenintegriteit te beschermen en aanvallen door een schadelijke hypervisor te voorkomen (zoals replay-aanvallen, herconfiguratie van het virtuele geheugenvertaalmechanisme, corruptie van geheugengegevens).

Het fundamentele principe van SEV-SNP is dat als een VM een geheugenpagina kan lezen die voor haar is gereserveerd (en daarom is versleuteld), ze altijd de laatste waarde moet lezen die ze zelf heeft geschreven. Verder vormen in het beveiligingsmodel dat voor SNP wordt gebruikt alleen de VM van de klant en de AMD-microprocessor onderdeel van de *trusted base*. Dit omvat niet de hypervisor, BIOS, andere VM's, enzovoort (zie Figuur 1). Tot slot stelt een SEV-SNP-optie VM's in staat om hun virtuele geheugen op te delen in vier *Virtual Machine Privilege Levels* (VMPL's) op een vergelijkbare manier als de beschermingsringen in de x86-architectuur.

AMD's attestatiemechanisme op afstand verifieert dat de hostmachine een AMD-processor is die de SEV-SNP-technologie ondersteunt en dat een VM is geïmplementeerd met SEV-SNP-bescherming. Elke AMD-processor bevat een beveiligde coprocessor die een paar dedicated sleutels genereert (*Platform Endorsement Key* of PEK), zelf ondertekend door een unieke sleutel die is afgeleid van geheimen opgeslagen met behulp van eenmalig programmeerbare zekeringen in de chip zelf. Deze PEK wordt ook indirect gebruikt om een gedeeld geheim te creëren tussen het SEV-platform en de klant.

Wanneer de beveiligde VM door de hypervisor op het SEV-platform wordt gestart, berekent de SEV-*firmware* de meting (waarde van de cryptografische hash) van het geheugen van de VM. Deze meting kan veilig worden doorgegeven aan de klant, zodat deze kan controleren of de uitgerolde VM niet is gewijzigd.

Intels SGX- en TDX-technologieën

Met Intels systeem *Software Guard eXtensions* (SGX), dat in 2015 werd geïntroduceerd, kan een software beschermde geheugengebieden definiëren voor beveiligde 'enclaves' die geïsoleerd zijn van andere processen die op dezelfde machine draaien (kernels van besturingssystemen, hypervisor, enz.) en waartoe randapparatuur ook rechtstreeks toegang heeft. De processor zorgt ervoor dat elke enclave zijn eigen speciale, versleutelde geheugengebied heeft en registreert elke allocatie door het besturingssysteem.

Een enclave wordt gegenereerd als een dynamisch gedeelde bibliotheek met behulp van standaard compilatietools. Wanneer een enclave wordt geïnitialiseerd, vraagt het besturingssysteem de processor om de toepassing te kopiëren naar geheugenpagina's in de versleutelde beschermde ruimte. Wanneer dan de toepassing in het geheugen is geladen, berekent de processor een meting van de toepassing. Hiermee kan vervolgens de integriteit van de toepassing gecontroleerd worden met behulp van een attestatiemechanisme.

In 2020 introduceerde Intel de technologie *Trusted Domain Extensions* (TDX), een ondertekende softwaremodule uitgevoerd in een nieuwe processormodus die kan worden gebruikt om virtuele machines te beschermen en cryptografisch te isoleren.

Er zijn twee soorten attestatie op afstand beschikbaar met SGX: *Enhanced Privacy ID* (EPID) en *Data Centre Attestation Primitives* (DCAP). De eerste is een attestatiemodus waarbij de Intel-attestatieserver moet worden gecontacteerd om informatie te verkrijgen over de aanvragende enclave. De tweede vereist geen contact met de Intel-attestatieserver.

Tijdens het bouwen van een enclave worden er twee metingen gedaan. MRENCLAVE is de cryptografische hashwaarde van de virtuele geheugenlayout die aan de enclave wordt toegewezen wanneer deze wordt gestart. De andere meting, MRSIGNER, is de cryptografische hashwaarde van de publieke sleutel van de auteur van de toepassing die in de enclave draait.

Hoewel SGX-technologie is verwijderd uit Intels twaalfde generatie Core-processors, blijft deze beschikbaar op derde generatie Xeon Scalable-processors [10]. Xeon Scalable-processors van de vierde generatie ondersteunen TDX-technologie en zijn verkrijgbaar bij Intels erkende partners en verdelers.

Herschrijven

We merken op dat het gebruik van SGX-technologie een grote herschrijving vereist van de bestaande toepassingen. Het is noodzakelijk om de toepassing te partitioneren door te bepalen welk deel van de code toegang moet hebben tot gevoelige gegevens. Hoewel deze essentiële stap complex is, verbetert het in principe de veiligheid van de toepassing, omdat algemeen wordt aangenomen dat een kleine toepassing – in dit geval een toepassing die in de enclave draait – minder kans heeft op fouten en gemakkelijker te verifiëren is dan een grote.

Communicatie tussen het beveiligde deel van de toepassing (binnen de enclave) en de rest van de toepassing (buiten de enclave) vindt plaats via aanroepen van functies die gedeclareerd moeten worden voordat de enclave wordt gelanceerd. Tenslotte kunnen toepassingen die geschreven zijn voor het SGX-platform niet gebruikt worden op andere platformen.

Meerdere leveranciers van publieke IT-infrastructuren bieden vandaag oplossingen voor *confidential computing* gebaseerd op TEE's. Hier beschrijven we de drie belangrijkste.

de code en gegevens van de klant tijdens de verwerking te beschermen tegen toegang van buitenaf. Amazon vertaalt dit in twee dimensies:

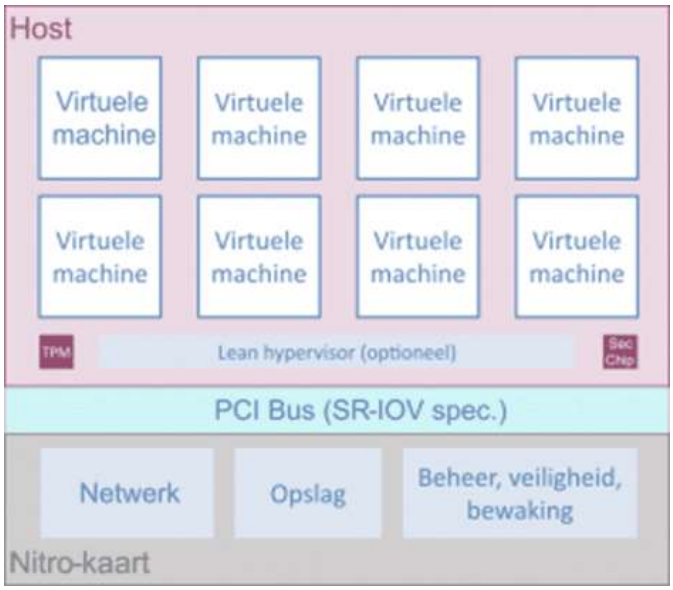
- Bescherming tegen de beheerder van de onderliggende IT-infrastructuur, in dit geval AWS;
- De mogelijkheid voor klanten om hun eigen workloads op te delen in meer of minder betrouwbare componenten, of om multi-agentsystemen te ontwerpen.

Amazon legt de nadruk op de architectuur van het Nitro-systeem, niet op de beschikbaarheid van een bepaalde microprocessor om een TEE te leveren. Sinds april 2023 biedt AWS echter ook de mogelijkheid om EC2-instanties te maken met AMD's SEV-SNP-technologie.

Het Nitro-systeem biedt volgens AWS geen enkel mechanisme waarmee systemen of personen verbinding kunnen maken met EC2-servers, het geheugen van EC2-instanties kunnen lezen of toegang kunnen krijgen tot opgeslagen gegevens. Onderhoudswerk kan alleen worden verricht via beperkte API's.

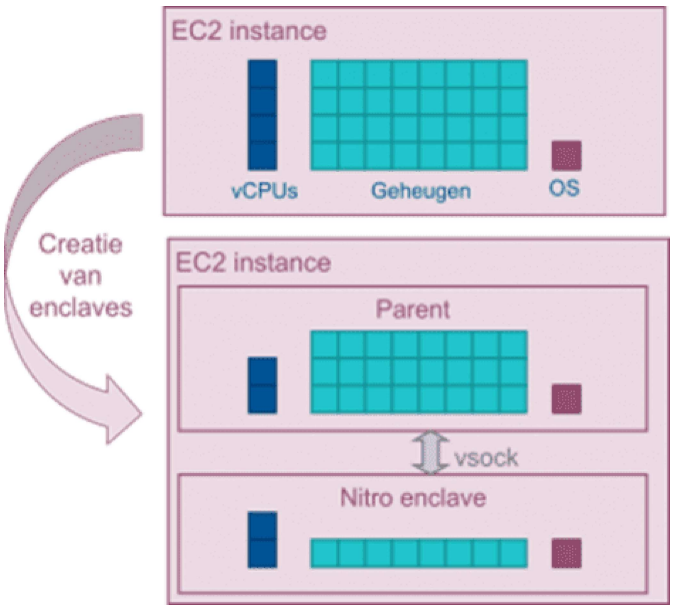
Het AWS Nitro-systeem (Figuur 2) is onderdeel van een herziening van Amazons infrastructuur voor EC2-servicevirtualisatie, inclusief het minimaliseren van de onderdelen van de hypervisor die op het moederbord draait. Het AWS Nitro-systeem is een combinatie van servers, processors, beheercomponenten en gespecialiseerde firmware die het onderliggende platform vormt voor alle Amazon EC2-instanties. Het bestaat uit drie hoofdcomponenten:

- **Specifieke Nitro Cards** – Hardwareonderdelen ontworpen door AWS die zorgen voor algehele systeemcontrole en I/O-virtualisatie onafhankelijk van het moederbordvan het systeem met zijn processors en geheugen;
- **Nitro-beveiligingschip** – Deze is geïntegreerd in het moederbord van de server en maakt veilig opstarten mogelijk op basis van een hardware root of trust, maakt het mogelijk om bare metal instances aan te bieden (waardoor de AWS-hypervisor overbodig wordt) en zorgt voor de bescherming van de server tegen ongeoorloofde wijzigingen in de firmware van het systeem;
- **Nitro-hypervisor** – Een geminimaliseerde, firmwareachtige hypervisor ontworpen om resource- en performance-isolatie te bieden.



Figuur 2 – Architectuur van een AWS-machine.

Nitro enclaves daarentegen zijn geïsoleerde virtuele machines die draaien op een klassieke EC2-instantie, een zogenaamde '*parent instance*' (Figuur 3).



Figuur 3 – Een Nitro enclave maken van een EC2 instance. Een enclave wordt gemaakt door de CPU en het geheugen van een EC2 instance, de zogenaamde parent instance, te partitioneren. Enclaves kunnen worden gemaakt met verschillende combinaties van processorcores en geheugen.

De belangrijkste beperking van Nitro enclaves is dat de toepassing die in de enclave draait geen verbinding heeft met het netwerk. Ze kan alleen communiceren met de parent instance via een point-to-point interface genaamd 'vsock', die wordt gedefinieerd door een context identifier en een poortnummer. Een eenvoudige '*lift and shift*' is daarom niet mogelijk.

Wanneer het is aangemaakt, kan de toepassing die in de enclave draait een asymmetrisch sleutelpaar genereren en de publieke sleutel in het certificaat laten opnemen. Hierdoor kan de *client-side* applicatie die het attest verifieert deze sleutel gebruiken om beveiligde communicatie met de enclave tot stand te brengen.

Microsoft Azure

Microsoft Azure stelt drie types *confidential computing* voor gebaseerd op TEE's:

- De **toepassingsenclaves** zijn gebaseerd op de SGX-technologie van Intel. Zoals eerder vermeld, is het noodzakelijk om de bestaande toepassingen grondig te wijzigen om ze aan te passen. Dit vereist veel denkwerk over welke delen van de toepassing beveiligd moeten worden en hun interactie met andere delen, maar het voordeel van deze aanpak is dat slechts een beknopte hoeveelheid code vertrouwd moet worden. Het nadeel is natuurlijk de complexiteit van de implementatie, die speciale training vereist voor analisten, architecten en programmeurs;
- De **confidential virtual machines** gebruiken AMD's SEV-SNP-technologie en Microsoft kondigde in april 2023 aan dat ze binnenkort Intels TDX-technologie beschikbaar zou stellen. Azure stelt tevens een '*trusted platform module*' (TPM) voor, die met name wordt gebruikt voor het attesteren van virtual machines;
- De **confidential containers** geven de klant een preciezere mate van controle over de TCB dan virtuele machines. In principe maakt dit verpakkingsmodel het mogelijk om bestaande containers in een SGX enclave te draaien zonder dat de software aangepast of opnieuw gecompileerd hoeft te worden (*lift and shift*).

De optie om meerdere threads parallel te laten draaien (*hyper threading*-technologie) binnen dezelfde processor is uitgeschakeld op alle SGX instances. Dit voorkomt aanvallen die leiden tot datalekken tussen toepassingen die dezelfde processor delen.

- **Confidential virtual machines** maken gebruik van AMD's technologie;
- **Confidential Kubernetes nodes** zijn ook gebaseerd op AMD's SEV-technologie. De Kubernetes engine van Google kan het gebruik van confidential virtual machines voor alle Kubernetes nodes afdwingen.

Terwijl alle confidential virtual machines virtuele TPM's bevatten die de integriteit van een virtuele machine valideren bij een gemeten opstart, bieden *confidential virtual machines* met SEV-SNP-technologie ook hardware cryptografisch ondertekende attestrapporten. SEV-SNP-technologie is echter nog niet algemeen beschikbaar op de infrastructuur van Google.

Praktische limiet van attesten

Een belangrijk punt bij het gebruik van TEE's is het verkrijgen van een garantie dat de software die draait op de gehuurde infrastructuur echt de software is die de klant verwacht en dat de gegevens die hij verwerkt niet kunnen worden gelezen door andere software. Deze garantie, een attest genoemd en verkregen via een betrouwbaar mechanisme, moet volledige, recente en semantisch expliciete informatie bevatten.

Ervan uitgaande dat we de fysieke veiligheid van de microprocessor of gespecialiseerde chip vertrouwen, dat bekende aanvallen zijn afgeweerd en dat de enclavecode niet kwetsbaar is voor side channel attacks, hoe kunnen we er dan zeker van zijn dat de output van een *enclave* betrouwbaar is?

Er moet voor gezorgd worden dat:

- **De binary file die in de enclave wordt uitgevoerd, gebouwd is met de verwachte code**. Hiervoor kan de klant zijn toepassing compileren op een vertrouwde machine (bijvoorbeeld een machine die hij bezit) en vervolgens de binary veilig kopiëren naar het confidential IT-platform. Een andere methode is om een *reproducible build system* te gebruiken;
- **De binary file die wordt uitgevoerd overeenkomt met het verwachte binary.** Een attestsysteem gebruikt cryptografische sleutels afgeleid van vaste geheimen in de vertrouwde microprocessor om een bewijs te ondertekenen dat de binary zich in een bepaalde toestand bevindt op echte hardware (geen simulatie). Het bewijs bevat een meting (cryptografische hashwaarde) van de binary;
- **De staat van de toepassing bij het starten** is de verwachte staat: het meten van het uitvoerbare deel van de binary is niet voldoende om het toekomstige gedrag te voorspellen;
- **Het attest is ondertekend door een vertrouwde entiteit**, in principe de fabrikant van de microprocessor of de beveiligde chip.

In de bestudeerde oplossingen, met uitzondering van SGX enclaves, wordt het attest echter ofwel ondertekend door de leverancier van de infrastructuur (en niet door de hardwarefabrikant), ofwel is het niet mogelijk om de meting van de beveiligde software te verifiëren omdat deze *proprietary libraries* bevat. Het risico bestaat dus dat de gecertificeerde entiteit liegt over haar status.

Conclusie

Tien jaar na de onthullingen van Edward Snowden in juni 2013, betreffende de Amerikaanse surveillancemethoden, moeten we ervan uitgaan dat informatie bemachtigd kan worden als deze voldoende waardevol is. De indruk dat nationale IT-infrastructuren veiliger zijn, kan daarom misleidend zijn.

nieuw argument ten voordele van publieke IT-infrastructuren.

Als ze correct worden geïmplementeerd, en alle andere zaken onveranderd blijven, kunnen TEE's op basis van fysieke componenten het niveau van gegevensbescherming binnen een IT-infrastructuur aanzienlijk verhogen, met name ten opzichte van derden en in het bijzonder cybercriminelen. Ze maken het in feite mogelijk om de meeste logische aanvallen te vermijden die conventionele systemen treffen, dankzij verbeterde procesisolatie, geheugenversleuteling via de hardwarelaag, veilig opstarten, controlemechanismen voor firmware-updates en, in het algemeen, een vermindering van de omvang van de trusted computing base. Met andere woorden, de veiligheidsmaatregelen opgenomen in de TEE's maken een aanval aanzienlijk complexer en duurder.

Het aanbod van op TEE-gebaseerde *confidential computing* varieert tussen leveranciers, afhankelijk van het type abstractie dat wordt aangeboden: software library, container, virtuele machine. De keuze van deze opties leidt tot verschillen in de omvang van de trusted code base (en dus het oppervlak dat blootgesteld wordt aan aanvallen), maar ook in de inspanning die nodig is om bestaande toepassingen aan te passen aan deze nieuwe omgevingen.

Bij het kiezen van een op TEE-gebaseerde oplossing voor *confidential computing* moeten daarom de volgende punten worden gecontroleerd:

- Bescherming moet verankerd zijn in de fysieke laag van het systeem en elk apparaat moet een unieke identiteit hebben;
- Het attestmechanisme moet het mogelijk maken om de inhoud te verifiëren van de TEE op onafhankelijke wijze van de infrastructuurleverancier;
- Het attest moet ten minste ondertekend worden door de fabrikant van de fysieke component en niet alleen door de infrastructuurleverancier;
- De dienst stelt ten minste in staat om eigen crypotografische sleutels te importeren in een toegewijde hardware-beveiligingsmodule (HSM), en in het beste geval om een eigen HSM te gebruiken;
- Het moet mogelijk zijn om de source code van de critical libraries die in de trust base zijn opgenomen door de infrastructuurleverancier te controleren op de goede werking van de klanttoepassing;
- De infrastructuurleverancier moet de klant een dienst ter beschikking stellen waarmee de verschillende software dependencies, compilatieomgevingen en binaries die voor de TEE worden gebruikt, kunnen worden getraceerd.

Tot slot is de gegevensbescherming aangeboden door *confidential computing* tijdens gebruik slechts één van de vele technische aspecten die in overweging moeten worden genomen met betrekking tot de vertrouwelijkheid van gevoelige gegevens (om nog maar te zwijgen van de juridische, economische en politieke aspecten).

Net zoals het beste slot op de voordeur van een huis het probleem van een wijd openstaande achterdeur niet oplost, gaat het gebruik van *confidential computing* ervan uit dat gegevens in rust en in transit effectief worden beschermd, maar vereist het ook specifieke training voor de mensen die verantwoordelijk zijn voor het aanpassen (in meer of mindere mate afhankelijk van het gekozen type *confidential computing*) en migreren van bestaande toepassingen, in het bijzonder analisten, architecten en programmeurs.

Dit is een ingezonden bijdrage van Fabien Petitcolas, research consultant bij Smals Research, gespecialiseerd in diverse Security-topics. Dit artikel werd geschreven in eigen naam en neemt geen standpunt in namens Smals. Interesse om bij Smals te werken? Neem dan een kijkje naar het huidige uitgebreide jobaanbod.

.gerelateerd nieuws

Introductie tot de nieuwe eHealth pseudonimiseringsdienst

Wave: Hoe Smals dossierbeheer bij RSZ herwerkte tot modulaire werkomgeving voor overheden

Intel maakt Gaudi 3 prijsbreker in zoektocht naar AI-relevantie

Geen hyperthreading voor toekomstige Lunar Lake Intel-CPU's

.nieuwsbrief

Abonneer je gratis op ITdaily !

naam@organisatie.com

☐ **Dagelijks** ☐ **Wekelijks**

Abonneren

◀ **terug naar home**

.populair

Meta gaat AI-systemen trainen met data Europese gebruikers

.data 07.06.'24 3 min

Wave: Hoe Smals dossierbeheer bij RSZ herwerkte tot modulaire werkomgeving voor overheden

.devops 11.06.'24 6 min

Microsoft bereid tot 'meer toegevingen' in Teams-antitrustzaak

.business 06.06.'24 2 min

Vermijd een hoge telefoonrekening in het buitenland met eSIM

.communicatie 07.06.'24 4 min

ITdaily is een B2B-platform met focus op IT-professionals en business decision makers. We laten hen kennismaken met innovaties, testen, verdieping, reportages en andere praktische verhalen. Via heldere teksten maken we complexe IT-verhalen toegankelijk.

- onze partners
- informatie & adverteren
- wire
- contact
- algemene voorwaarden
- privacybeleid