SAP-systemen **onnodig** onveilig

SAP-gebruikers vaak niet bewust van de risico's

De waarde van de informatie die in de SAP-systemen is opgeslagen is enorm. Toch is deze data vaak veel slechter beveiligd dan het doorsnee kantoorsysteem. De complexiteit van deze installaties is de belangrijkste oorzaak. Maar de gebruiker zou om te beginnen eens wat beter kunnen patchen.

door: TANJA DE VREDE / T.D.VREDE@AUTOMATISERINGGIDS.NL **beeld:** ANTHONY DONNER / ANTHONYDONNER.COM

Met zeker 180.000 klanten wereldwijd, waaronder ruim driekwart van de bedrijven uit de Forbes 500-lijst, is SAP een uiterst populair zakelijk systeem. En niet alleen onder de gebruikers, maar ook onder computercriminelen. De waarde van de informatie die in de SAP-systemen is opgeslagen is enorm. En tegelijkertijd zijn die systemen slecht beveiligd. Slechter dan het doorsnee kantoorsysteem.
Joris van de Vis, Robin Vleeschhouwer en Fred van de Langenberg, samen oprichters van ERP Security, zijn gespecialiseerd in de beveiliging van SAP-systemen. Zij wijzen op de enorme complexiteit van SAP-installaties die het erg moeilijk maken de systemen goed te beveiligen. Van den Langenberg: "Ik vind het schokkend dat we bij elke klant waarvan we de beveiliging testen, binnen enkele minuten binnen zitten."
Tot zo'n tien jaar geleden draaiden de meeste SAP-systemen nog in een intern netwerk dat niet verbonden was met internet. Nu zijn vrijwel alle applicaties van SAP via het web toegankelijk. SAP-portals, SRM's en CRM's zijn op afstand te benaderen. Met SAP XI worden verschillende bedrijfsvestigingen verbonden. Via SAP Router zijn bedrijven verbonden met SAP zelf. En dat biedt onverlaten kansen op die systemen in te breken.

Veel oude versies

Extra kwetsbaar zijn deze systemen doordat er nog veel oude versies in gebruik zijn. Zo draait NetWeaver 7.0 EHP – dat in 2005 uitkwam, door klanten zeer traag wordt geüpdatet en veel lekken bevat – nog op 35 procent van de SAP-servers, zo blijkt uit onderzoek van het Amerikaanse ERPScan. Het bedrijf zocht en vond met behulp van Google en de gespecialiseerde zoekmachine Shodan moeiteloos vele servers met oudere versies van SAP-applicaties die via internet toegankelijk zijn. En dus makkelijke prooien voor computercriminelen, want die scannen net zo makkelijk automatisch op SAP-servers die met het web zijn verbonden.
De drie experts in SAP-beveiliging wijzen ook op de gevaren van binnenuit. "Een insider kan alles. Neem standaard systemen waarbij alles default open staat. De eigenaar van de database die kwaad wil kan alle gegevens kopiëren van elke tabel, rekeningnummers aanpassen, zelf gebruikers aanmaken, Dos-aanvallen initiëren en fake bestellingen aanmaken. Of dat geheime recept kopiëren van die bierbrouwer waar hij werkt en die dat gewoon in zijn SAP-systemen heeft opgeslagen."
Volgens Van de Vis kiezen veel gebruikers voor SOD – segregation of duties – als bescherming. "Ze timmeren hun systemen dicht met autorisaties en krijgen zo een rolgebaseerde toegangscontrole. Dáár richten ze al hun beveiligingsinspanningen op. Dat is de klassieke methode om hackers tegen te houden. Dat is ook goed onderhoudbaar maar dat is niet meer genoeg. Want een deskundige hacker kan die autoristatiestructuur omzeilen. SAP heeft 3 lagen: de applicatielaag waar SOD in zit, het besturingssysteem en de databases. SOD zit in die applicatielaag maar de onderliggende infrastructuur is daarmee niet beschermd. Want je kunt via het besturingssysteem overal in."

Vijf jaar achter

SAP neemt wel degelijk beveiligingsmaatregelen, erkennen Vleeschhouwer, Van de Vis en Van de Langenberg. "Maar daar loopt het wel zo'n vijf jaar in achter op bedrijven als Microsoft. Het is ook moeilijk voor SAP om uniforme richtlijnen te maken want er zijn zeer veel verschillende SAP-systemen: ERP-types, XI, BI- en CRM-oplossingen. Daarbij speelt ook nog dat SAP op diverse besturingssystemen draait en met verschillende databases werkt waardoor SAP-omgevingen flink van elkaar verschillen."
SAP heeft ruim 200 security guidelines uitgebracht. "Maar dat leest dus niemand. SAP biedt wel de mogelijkheden, maar het is een overload aan guidelines. Daarnaast speelt mee dat veel gebruikers zich niet bewust zijn van de risico's die ze lopen", zegt Van de Vis.
Niettemin blijft het feit staan dat SAP dus wel degelijk in security

Tips

Door de complexiteit van de SAP-systemen, die verspreid kunnen zijn over verschillende besturingssystemen, servers, virtuele servers en databases is het volgens Vleeschhouwer, Van de Vis en Van de Langenberg erg moeilijk om dit vanuit de infrastructuur te beveiligen. Maar wat moet een SAP-gebruiker dan doen om zijn beveiliging enigszins op orde te krijgen?

- **Zorg voor een baseline met eenvoudige maatregelen. Iets eenvoudigs als een password dat minimaal tien karakters moet bevatten is al een enorme verbetering. Maar breng eerst de risico's in kaart.**
- **SAP heeft vorig jaar een gids uitgebracht met een top 10 van belangrijkste beveiligingsproblemen en –oplossingen. Als je die in acht neemt, dek je een groot deel van de risico's af.**
- **Zorg eerst voor awareness en zie dat je van het hoogste niveau mandaat krijgt. Kijk dan wat de kwetsbaarheden zijn en welke maatregelen het meeste opleveren. Bepaal ook welk risico je wilt lopen.**

FRED VAN DE LANGENBERG (LINKS), ROBIN VLEESCHHOUWER (MIDDEN) EN JORIS VAN DE VIS:
“SAP LOOPT IN HAAR BEVEILIGING ZO’N VIJF JAAR ACHTER OP BEDRIJVEN ALS MICROSOFT.”

guidelines vrijwel alle bij haar bekende beveiligingsproblemen heeft gedocumenteerd en er oplossingen voor biedt. Ook staan in nieuwe versies van SAP-modules poorten vaker default dicht. Tot enkele jaren geleden stonden ze default open, maar dat is nu langzaam aan het veranderen. Nadeel is wel dat veel gebruikers nog oude versies hebben draaien, waarin dit nog wel het geval is. Daarbij komt dat veel gebruikersorganisaties de updates waarin veel lekken worden gedicht, domweg niet doorvoeren. Van de Langenberg: “Er staat veel legacy. Het is lastig om daar wijzigingen in door te voeren. Het risico dat je dingen verstoort met de vaak grote support packs is groot. Dat moet dus eerst goed getest worden en dat kost tijd en geld en energie. En loop je eenmaal achter, dan haal je dat niet meer in.”

Updaten moeilijk

Ook ERPScan stelt dat het niet het probleem is dat er geen patches zouden zijn. Die zijn er. En SAP ondersteunt versies uit 2005 ook nog. Het gaat er meer om dat klanten het te moeilijk vinden om de systemen te updaten. Daarnaast vinden de drie ondernemers dat er weinig kennis is over beveiliging. “Weinig mensen weten hoe je het goed dicht zet. Er zijn basisconstructies voor het installeren en patchen, maar ‘hardenen’ van de systemen is binnen organisaties vaak een speelbal tussen afdelingen – dat wordt zelden goed belegd. En dan speelt ook nog dat maatregelen die de business kunnen hinderen heel snel geweigerd worden, vanwege de mogelijke impact. Dat is een probleem. Je moet om dat enigszins te voorkomen, zorgen dat je zo hoog mogelijk in de organisatie steun krijgt.”

SAP lijkt zich wel bewust van dit probleem en probeert ook gebruikers wat beter aan het patchen te krijgen. “We hebben onze strategie gewijzigd met als doel het voor klanten zo makkelijk mogelijk te maken om de hoogste release te hebben”, zegt een woordvoerder van SAP Nederland. “In het verleden was dat nogal eens lastig. Wij gaan nu uit van een stabiele core waarin weinig verandert. We hebben de boel losgeknipt: je kunt de nieuwe release installeren zonder dat je nieuwe functionaliteit moet gebruiken. En het merendeel van onze klanten zit nu op die nieuwe releases. Je krijgt business suite 7 en daar zitten packages in. Maar je kunt klanten niet dwingen te upgraden. Dat bepalen ze zelf. Wij kunnen het ze alleen maar zo makkelijk mogelijk maken.”

SAP biedt ook trainingen aan op het gebied van security. Maar massaal worden deze niet bepaald bezocht. In 2012 volgden in Nederland 50 deelnemers cursussen als SAP System Security The Fundamentals en Security in an SAP System Environment. Dit jaar waren het er tot de zomer 33.