

— VOORZORGSMAATREGELEN —

Robuuste
toepassing
cryptografie

Als de volgende voorzorgsmaatregelen worden genomen, is het oplopen van grote schade door het onbruikbaar worden van cryptografie belangrijk te verminderen.

■ Bij het systeemontwerp rekening houden met het op een bepaald moment moeten vervangen van het algoritme. Dat betekent dat het programmadeel met het algoritme vervangbaar moet zijn. Oog houden op de ontwikkelingen in de techniek is onontbeerlijk, immers in laboratoria over de hele wereld wordt geprobeerd nieuwe cryptografische algoritmen te ontwikkelen en bestaande te kraken. Het zal nodig kunnen zijn om gedurende enige tijd twee algoritmen naast elkaar te laten bestaan. Het is van belang een migratiescenario op te stellen om de overgang van de ene naar de andere implementatie uit te voeren.

■ Een roadmap maken voor het vervangen (of veranderen) van sleutels. Het slechtste moment om sleutels te vervangen is wanneer zij bekend (gecompromitteerd) zijn. Vanaf dat moment werkt de beveiliging immers niet meer. Indien mogelijk zal het vervangen van sleutels dan ook gebeuren op het moment dat de oude nog bruikbaar zijn. In deze situatie is niet alleen het vervangen van de sleutels belangrijk maar ook het genereren en transporteren ervan. Het is dus zinnig voor beide situaties scenario's of roadmaps te ontwikkelen. Bij voorkeur lang voordat het nodig is.

■ Een roadmap maken voor het vervangen van het algoritme. De operatie om de cryptografische functie te vervangen door een ander algoritme, is ingrijpend. Immers, de cryptografie is de kern van de beveiliging van het systeem. Het zal niet mogelijk zijn die functie er even niet te laten zijn. Het overstappen van de ene naar de andere implementatie zal zorgvuldig voorbereid moeten worden om te voorkomen dat er onveilige situaties ontstaan.

■ Calamiteiten/crisisplan opstellen voor het geval dat de gebruikte cryptografie plotseling onbruikbaar wordt. Dat kan zijn omdat het algoritme gekraakt is, omdat de sleutels bekend geworden zijn of omdat met andere technieken het mogelijk wordt de beveiliging te doorbreken. Er is in dit geval sprake van een ernstige calamiteit. Immers, alle deuren staan ineens open en het zal enige tijd vergen om ze weer te sluiten.

Cryptografie beperkt houdbaar

Business Continuity Management, in combinatie met cryptografie, moet bedrijfsprocessen veiligstellen

De afhankelijkheid van cryptografie is enorm, maar de houdbaarheid ervan is beperkt. Dat wil zeggen, er komt een moment waarop een algoritme niet meer bruikbaar is, bijvoorbeeld omdat het is gekraakt of omdat er te veel zwakke plekken in zitten. **Jacques Cazemier** en **Christ Reniers** nemen de stappen door die gezet moeten worden om calamiteiten te voorkomen.

Wie zijn auto met een afstandsbediening opent met een draadloze sleutel 's morgens binnenkomt op kantoor, gebruikt cryptografische technieken. Daar merk je niets van, dat is een onderdeel van de sleutel. Maar niet alleen voor fysieke beveiliging gebruikt men cryptografie: de bedrijfsvoering van organisaties (groot en klein) is 'onder water' inmiddels afhankelijk van cryptografie. Bijvoorbeeld het veilig omgaan met wachtwoorden in een netwerk is mogelijk omdat de wachtwoorden versleuteld worden verstuurd en opgeslagen. Mo-

Bij systeemontwerp al rekening houden met vervangen algoritme

biele telefonie en satelliet-tv gebruiken cryptografie voor hun chipkaarten. Ook voor veilig internetbankieren wordt cryptografie gebruikt evenals bij thuiswerken via internet. Verder kunnen alle acties met pinautomaten en betaalautomaten (ATM) op straat niet zonder vormen van cryptografie. Stel je voor dat die cryptografie vanaf dit moment niet meer werkt. Dan werken al die functies niet meer. Dat kan gebeuren op het moment dat in een laboratorium of op een zolderkamer het cryptografische algoritme is gekraakt. Cryptografie is ongemerkt een onlosmakelijk deel van onze maatschappij geworden. We gebruiken dagelijks cryptografie zonder daar bij stil te staan. Onze beveiliging is er in veel gevallen van afhankelijk. Het ontbreekt ons niet alleen aan overzicht waar en hoe we cryptografie

gebruiken, maar we onderschatten ook de gevolgen ervan. Een belangrijk gegeven van het gebruik van cryptografie is dat de houdbaarheid ervan beperkt is. Dat wil zeggen dat er een moment komt waarop een algoritme niet meer bruikbaar is. Omdat het gekraakt is, omdat er te veel zwakheden in zijn ontdekt, of omdat het mogelijk geworden is om alle mogelijke sleutels uit te proberen.

Eind jaren zeventig van de twintigste eeuw, toen het cryptografisch algoritme DES werd ontwikkeld, ging men ervan uit dat dit algoritme met een sleutelengte van 56 bits, rekening houdend met de wet van Moore, tot 1990 veilig zou zijn. Kostte een machine in 1977 om DES te kraken tussen de 20 en 50 miljoen dollar, dat kan tegenwoordig al met hardware van 2.000 of 3.000 euro. De internationale gemeenschap heeft dit gevaar onderkend en heeft DES vervangen door AES, een nieuw openbaar cryptografisch algoritme waarvan men verwacht dat het met de voortschrijdende technologische ontwikkelingen de komende tien tot vijftien jaar nog niet gekraakt kan worden. De grote afhankelijkheid van cryptografie in ons dagelijkse leven betekent dat we daar ook bewust mee moeten omgaan. Het toepassen van cryptografie voor bescherming van een bedrijfsproces, is een afweging tussen de beschikbare technologie en het algoritme dat met deze technologie nog voldoende sterk geïmplementeerd kan worden. Bij nieuwe systeemontwikkelingen moet rekening worden gehouden met de beperkte levensduur. Hoe langer een algoritme in gebruik is, hoe groter de kans dat iemand erin slaagt het algoritme te kraken. Het kraken van een cryptografisch algoritme dat men gebruikt voor beveiliging van bedrijfsprocessen kan men beschouwen als een calamiteit. Een dergelijke techniek wordt immers alleen gebruikt voor de bescherming

van die functies die echt belangrijk zijn. Uitval ervan zal grote invloed hebben. Niet in de laatste plaats op het gebied van imago en vertrouwen.

Business Continuity Management (BCM) is een middel om in geval van calamiteiten de vitale bedrijfsprocessen zoveel mogelijk te beschermen. Er is inmiddels veel ervaring opgedaan met het inrichten ervan, in het opzetten van crisismanagement en het opstellen van plannen om na een calamiteit zo snel mogelijk weer operationeel te zijn. Onderdeel van BCM is ook het tref-

Sleutels vervangen als de oude nog bruikbaar zijn

fen van voorbereiding om bij een calamiteit minder schade op te lopen. Daarbij gaat het niet alleen om het inrichten van een crisiscentrum maar ook om het robuust inrichten van de toepassing van cryptografie. Veel organisaties hebben inmiddels ervaring met BCM. Met name in de financiële sector is er, dankzij de regelgeving van de Nederlands bank, veel gedaan op dit gebied. Bij het grootste deel van die inspanningen waren het echter de zakelijke processen die aandacht kregen. Het is aan te raden cryptografie bij het toepassen van BCM mee te nemen.

Jacques A. Cazemier en Christ Reniers zijn als managementconsultants werkzaam bij Verdonck, Klooster & Associates (VKA). Beiden hebben jarenlange ervaring met informatiebeveiliging en BCM.



ILLUSTRATIE: GETTY IMAGES

— ONTWERPWEDSTRIJD —

Nieuw algoritme

Op 1 november zijn ongeveer veertig ontwerpen ingediend voor een nieuw algoritme voor het uitvoeren van de hash-functie. Dergelijke cryptografische functies worden onder meer gebruikt bij het zetten van elektronische handtekeningen. Het NIST had de wedstrijd uitgeschreven omdat sommige van de huidige familie van hashfuncties zwakker bleken dan was

aangenomen. Zo is het SHA-1 (Secure Hash Algorithm) in 2005 – onverwacht – in een Chinees laboratorium gekraakt. Dit is het meest recente voorbeeld van beperkte houdbaarheid van cryptografie. Er is een nieuw algoritme nodig omdat het huidige niet meer sterk genoeg is. Het creëren en testen van zo'n algoritme kost veel tijd. Begin volgend jaar wordt bekend-

gemaakt welke algoritmen op de shortlist komen. Dan wordt met name op universiteiten geprobeerd de algoritmen te kraken. Het overblijvende algoritme zal dan in 2012 officieel als standaard worden gepubliceerd.

➤ Voor meer informatie zie: <http://csrc.nist.gov/groups/S1/hash/sha-3/index.html> en <http://www.schneier.com/skein.html>.

— BEVEILIGING —

Vijf stappen

De stappen die uitgevoerd moeten worden om te voorkomen dat het gebruik van cryptografie als mechanisme van beveiliging meer na- dan voordelen oplevert:

■ **Stap 1: Premisse**
Aangenomen wordt dat de implementatie van de cryptografische functie zodanig is, dat het mogelijk is zonder al te veel inspanning updates uit te voeren. Zo'n update bestaat in eerste instantie uit het vervangen van sleutels in tweede instantie uit het vervangen van de implementatie van het algoritme. Als het niet mogelijk is dat zonder veel inspanning uit te voeren, dan is de eerste taak om stappen te ondernemen dat te verbeteren.

■ **Stap 2: Inventarisatie en prioriteiten**
Van alle systemen, applicaties, servers et cetera waar de cryptografische functie in aanwezig is, moet bekend zijn waarvoor zij dient, welke processen of functies daarvan afhankelijk zijn. Daarna moet – in overleg met gebruikende organisatiedelen – vastgesteld worden hoe belangrijk dat is. Er moet immers een lijst komen met de volgorde van behandeling. Verder kan dit dienen om fasering mogelijk te maken en zelfs om paralleltrajecten voor updates te kunnen inrichten.

■ **Stap 3: Organisatie**
De uitvoering van de update vergt organisatie. Soms gaat het daarbij om het ontwikkelen en uitrollen van software op beperkte schaal, soms is het omvangrijker en moeten sleutels vervangen worden op tientallen locaties, bij voorkeur in zo kort mogelijke tijd. De vorm en omvang van de organisatie zijn dan ook afhankelijk van de karakteristieken van de update. Op het moment dat die details bekend zijn – de gegevens uit stap 2 zijn daar ook voor nodig – is het mogelijk de organisatie vorm te geven. Een onderdeel kan zijn een crisisteam dat met veel mandaat in staat is bij escalatie knopen door te hakken. De organisatie kan verder gebruikt worden om voorbereidingen te treffen voor de uitvoering van de update.

■ **Stap 4: Documentatie**
Het is mogelijk dat er inmiddels verschillende scenario's ontwikkeld zijn om updates of delen daarvan uit te voeren. Het is noodzakelijk die uitwerkingen vast te leggen. Welke vorm de documenten hebben, is niet van belang; de ene organisatie gebruikt handboeken, de andere plannen. Vooral escalatie en omgaan met kleine of grote calamiteiten verdienen aandacht omdat het handig is de uitwerking gedaan te hebben voordat een escalatie plaatsvindt.

■ **Stap 5: Oefenen**
Het uitvoeren van een dergelijke update is een taak die niet regelmatig voorkomt. Het is noodzakelijk om een team als team te laten opereren. Dat geldt met name voor het crisisteam. Ervaring met Business Continuity Management heeft geleerd dat bij oefeningen de onvolkomenheden aan het licht komen.

➤ Voor reacties en nieuwe bijdragen van deskundigen: Henk Ester (h.ester@sdu.nl), (070) 378 03 97).