In deze rubriek geven enkele IB-redacteuren in een kort stukje hun reactie op recente nieuwsitems over informatiebeveiliging. Dit zijn persoonlijke reacties van de auteurs en deze geven niet noodzakelijkerwijs het officiële standpunt weer van hun werkgever of van PvIB. Vragen en/of opmerkingen kun je sturen naar ibmagazine@pvib.nl.

Waar komt nou echte innovatie op het gebied van informatiebeveiliging vandaan?

Op veel vlakken van de informatie technologie is het duidelijk wie de aanjager is van innovaties. De ontwikkeling van Graphics Processing Units (GPU's) was bijvoorbeeld niet mogelijk geweest zonder de gaming industrie.

Chris Miller beschrijft in zijn fascinerende boek Chip War (1) hoe de innovatie van Central Processing Units (CPU's) altijd gedreven is door de defensie industrie. Dat begon al eind jaren 50 van de vorige eeuw in de Koude Oorlog. Maar ook in de Vietnamoorlog was de ontwikkeling van rekenkracht cruciaal. In het begin waren bombardementen (zoals Operation Rolling Thunder van 1965 tot 1968) gebaseerd op 'spray' en 'pray' met een marginale impact. Texas Instruments was het eerste bedrijf dat begin jaren 70 de microchips ontwikkelde voor geleide wapens, met een voor die tijd ongekende precisie. Met een cynische blik zou je kunnen zeggen dat de oorlog in de Oekraïne een proeftuin is voor AI-geleide wapens die zelfstandig hun doel zoeken.
Informatiebeveiliging is natuurlijk een veel oudere wetenschap. De behoefte om informatie te beveiligen, is waarschijnlijk zo oud als de mensheid zelf. Iedereen kent Caesar's cipher uit de schoolboeken, de eerste gedocumenteerde encryptiemethode.

Wordt echte innovatie nou geïnitieerd door de 'good guys' of de 'bad guys'? Of maken we het de bad guys zo gemakkelijk omdat security vaak nog het vijfde wiel aan de wagen is bij de ontwikkeling van een nieuw product?

Alex Dingemanse - Stem met je voeten

Nieuwsgierigheid zit diep in ons brein gebakken. Zonder deze eigenschap had de mensheid nooit de ontwikkeling meegemaakt zoals we die hebben meegemaakt. Ik kan me nog herinneren dat ik begin jaren 90 van de vorige eeuw de eerste spam mails toch wilde lezen; je wist immers maar nooit of er iets interessants in zou staan. Het heeft mij heel wat discipline gekost om het spiergeheugen te trainen om verdachte e-mails ongelezen te verwijderen.

En heb ik nou echt dat connected koffiezetapparaat nodig? Of is het een onnodige gadget waarbij het niet ondenkbaar is dat er een hardcoded admin-password wordt gebruikt. Alles dat Internet toegang heeft, kan worden gehackt.

We zijn nog steeds jagers-verzamelaars. Alleen verzamelen we nu apps, likes en volgers. In een studie uit 2019 van meer dan 82.000 voorgeïnstalleerde Android apps van 1.700 modellen van 214 merken, bleek dat deze telefoons buitengewoon onveilig waren (2). Volg de adviezen van Carissa Véliz (3) en maak je eigen privacy tot een prioriteit. Maak er een gewoonte van om geregeld apps van je telefoon te verwijderen als blijkt dat je ze toch niet gebruikt.
In een zakelijke omgeving moeten leveranciers bereid zijn om openheid van zaken te geven. En sorry, het standaardant-

Maarten Hartsuijker | Alex Dingemanse | Fook Hwa Tan

woord: 'we kunnen een SOC 2 Type 2 rapport delen', is gewoonweg niet voldoende. Maar misschien nog wel erger zijn de vele pagina's met van het internet gekopieerde detailvragen in aanbestedingen die niet ter zake doende zijn. Het zegt vaak meer over de gebrekkige kennis van de schrijver en ze hebben zelden toegevoegde waarde. Het maakt vaak pijnlijk duidelijk dat Informatiebeveiliging een vak apart is. Heb je de kennis niet, koop die dan in. Want alleen als je je eisen goed kunt formuleren kun je de juiste productkeuze maken. Maak beveiliging een van de standaardeisen in alle componenten van je IT-omgeving. En durf 'nee' te zeggen en weg te lopen, als je niet bent overtuigd.
En wat de koffie betreft: ga voor de kwaliteit van je bakkie troost en weiger je apparaat op je wifinetwerk aan te sluiten, de smaak wordt er niet beter van.

Maarten Hartsuijker - Basale fouten

Nieuwe technische snufjes zijn mooi, maar wellicht winnen we nog wel het meest met de innovatie van onszelf. Door nauwgezetter de basis op orde te brengen en te houden. Je kunt 10-factor authenticatie toepassen, maar als je IDP de bescherming van zijn sleutelmateriaal niet op orde heeft dan maak je het vooral je gebruikers moeilijk. Je kunt de meest intelligente applicatie firewalls plaatsen, maar als een groot deel van de communicatie er vervolgens gecodeerd doorheen wordt gesluisd dan had je dat dubbeltje beter anders kunnen besteden. Je kunt een slim versleuteld communicatiesysteem met sterke encryptie voor hulpdiensten ontwikkelen, maar als je de sleutels van weinig willekeurigheid voorziet of zelfs hergebruikt dan faalt zelfs de allersterkste cryptografie. We zijn met z'n allen jarenlang redelijk weggekomen met 'slordig' beveiligingswerk. Helaas lijken de bedreigingen (noem het innoverende bad guys) nu sneller toe te nemen dan we onze kwetsbaarheden kunnen verminderen (de innoverende good guys). Met een toenemend risicoprofiel tot gevolg. Die balans zien we natuurlijk liever weer de andere kant op doorslaan...

Fook Hwa Tan - Informatiebeveiliging en de cruciale rol van chipontwikkelingen in moeilijke tijden

In tijden van toenemende digitale afhankelijkheid worden informatiebeveiliging en chipontwikkelingen steeds essentiëler. De snelle opkomst van technologie en de groei van cyberdreigingen vragen om innovatieve maatregelen om onze gegevens te beschermen. In deze context spelen ontwikkelingen op het gebied van chips een cruciale rol in het waarborgen van een veilige digitale omgeving.
Chips vormen de ruggengraat van elk elektronisch apparaat. Ze zijn verantwoordelijk voor het verwerken en opslaan van gegevens. Met de groeiende complexiteit van cyberaanvallen moeten chips zich aanpassen om geavanceerde versleutelingsmethoden en beveiligingsprotocollen te ondersteunen. Dit vereist nauwe samenwerking tussen fabrikanten, cybersecurity-experts en beleidsmakers om ervoor te zorgen dat alle veiligheidsaspecten in acht worden genomen. In tijden van crisis, denk aan de COVID-19-pandemie, vertrouwen we nog meer op digitale technologieën om te blijven functioneren. Het massale thuiswerken en het dito gebruik van online diensten vergroot echter het aanvalsoppervlak voor cybercriminelen. Waardoor de ontwikkeling van robuuste, veilige chips nog urgenter wordt. Naast hardwarematige oplossingen spelen ook softwarematige beveiliging en bewustwording bij gebruikers een belangrijke rol. Een geïntegreerde aanpak waarbij chips fungeren als veilige toegangspoorten en waarbinnen gegevensversleuteling centraal staat, is de sleutel tot een betere bescherming tegen datalekken en cyberaanvallen.
Een ander aspect dat aandacht verdient, is de bescherming van persoonlijke gegevens in het Internet of Things (IoT)-tijdperk. Aangezien steeds meer apparaten verbonden zijn, moeten chips in deze apparaten ook voldoende beveiliging bieden om te voorkomen dat ze worden gemanipuleerd of misbruikt voor kwaadwillende doeleinden.
Concluderend: in tijden van moeilijkheden krijgt informatiebeveiliging een hogere prioriteit dan ooit tevoren. Chipontwikkelingen spelen een cruciale rol in het waarborgen van een veilige digitale omgeving. Door te investeren in geavanceerde chips met ingebouwde beveiligingsmechanismen, kunnen we de toenemende dreigingen effectief het hoofd bieden en het vertrouwen in onze digitale samenleving behouden. Samenwerking tussen alle betrokken partijen is essentieel om deze uitdaging aan te gaan en een robuuste, veilige toekomst te waarborgen.

Referenties

(1) Miller, C. (2022). Chip War. The fight for the world's most critical technology. Simon & Schuster, Inc.

(2) Gamba, J., Rashed, M., Razaghpanah, A., Tapiador,J., and Vallina-Rodrigeus, N. (2019). An Analysis of Pre-Installed Android Software', 41 IEEE Symposium on Security and Privacy

(3) Véliz, C (2021). Privacy Is Power. Why and How You Should Take Back Control of Your Data. Melville House Publishing