CR056

Digital certificate revolution with Nick France, Sectigo

Capgemini

CR056

Digital certificate revolution with Nick France, Sectigo

Disclaimer: Please be aware that this transcript from the Cloud Realities podcast has been automatically generated, so errors may occur.

[00:00:00] Can I just say, uh, sorry, I can't do this podcast because we're recording with somebody from the wrong side of the Pennines. So I think I'm going to have to, uh, exit stage left. I'm very sorry. I'd like to question that wrong side part, but okay.

Welcome to Cloud Realities, a conversation show exploring the practical and exciting alternate realities that can be unleashed through cloud driven transformation. I'm David Chapman. I'm Sjoukje Zaal, and I'm Rob Kernahan.

And this week we're going to be delving into both the niche, but really critical area of digital certificates.

These are the things that underpin pretty much all the security on the internet and big changes are coming. So today we're going to have a look at that world and dig into what organizations need to do to start to respond to the big [00:01:00] changes that are on the way. But before we get to that,

I was in the office the other day and Rob had had a number of. What looked like code cracking books out on his desk and I went over to him and I'm like, Rob, what are you up to this week? And he said, well, I'm trying to work out the effect that quantum is going to have on the world of encryption, David.

And, and, and it's taking some time. It's taking more time than I expected. And I'm like, wow, I'm not surprised Rob, not using the, not using those code cracking books anyway. And he said, but I'm also thinking about this other thing. And I said, Rob, what else is confusing you this week? Uh, uh, yes, David. Yes, I remember it well.

Um, but there are a good read in the evening code cracking, so off you go. Yeah, it good. But the, the, uh, the other thing that was confusing me, David, was the, what's gonna happen between Apple and the eu? Um, with the digital market, it's looming close, right? So what you've got is the [00:02:00] EU's gone. You've got to open up your platform.

So digital markets act came out 2022 and said, you know, by March, you've got to sort all this stuff out to be fair. Apple have, however, Apple's implementation of meeting the digital markets act, which will essentially allow third party app stores in and third party payment providers. is to basically create a situation that so financially disadvantages you, uh, to use these third party systems that you would never use them.

So things like, um, uh, over a million downloads, no matter what, if you're monetized app or not, you have to pay 50. cents. Uh, and then, uh, there's still a 17 percent levy on payments and you need a million dollar letter of credit to do it and all this sort of stuff. And they've even published a calculator in whichever way you cut it.

Lots of organizations have complained and the best one was Epic Games CEO Tim Sweeney described it as hot garbage, which I thought was quite a [00:03:00] nice way to describe it, right? So what have Apple done? We've complied with the law, but done it in such a way that Nobody's ever going to be able to actually implement what the law is trying to do.

So basically everybody's complaining, they're up in arms. I think they're all lobbying EU has basically said, well, we'll wait till the date kicks in for the Marks Act. And then if there is action to be taken, it will be taken. So you can expect there's likely to be quite a swift response because they've obviously gone out of their way to make it high friction and very complicated.

And so I am very confused about who's going to win because at the same time, you've got big tech and versus. Government, EU, big market, 450 million people, but in the US as well, Department of Justice is also looking at Apple for anti competitive practices as well. So they

might get them into a lawsuit and you think, wow, big tech versus government, what's going to happen?

You know, it's a difficult one, isn't it? And it comes with scale will be my initial observation, which is it's sort of. Any organization's right to create an [00:04:00] ecosystem that's closed and you know that you can either opt into that so you know I opt in like I've got my phone's an iPhone and I don't mind because on a day to day basis I don't really want to think about like what app store should I use and what this and what that so I'm quite happy with the customer experience design centric element of what Apple do.

And they do it, you know, as good as if not better than most organizations in the world today. Um, a pinnacle of it, if you like. Now, when does that move from being a design principle and in control of a company to being something that's so scaled that it becomes monopolistic and anti competitive? And it's interesting as a conversation, and it is difficult to Pin down because it also gets into the point of tech companies generally are just getting so big and can make decisions that can impact forward and [00:05:00] have ripple effects that are massive.

So I would say yes, it's going to be interesting to watch the Apple case study. And that's going to have ramifications for Apple and therefore the usership of Apple. But I wonder if it's going to have even wider ramifications of that about the grip of tech generally. Yeah, I think I think a nation states organizations I think have been nervous to take on big tech and we had this in the taxation argument and global tech tax and things like this.

But I do feel this is a watershed moment and it'll go one way or the other and it might just Peter out and it is what it is, or actually it might force. real change. But you're right about when you get to a de facto standard of size and scale, uh, you know, and you've only got two choices. I do think there is an argument, say some regulators there, but there is the other argument around protecting the consumer to say, whilst it's in the same ecosystem, you can assure it much more easily.

So there's, there's two sides to it. I know my kids were, uh, livid when, uh, Epic Games pulled [00:06:00] out and took Fortnite off the, uh, of the iOS platform. And they've been one of the ones spearheading this, and I know Spotify are, are also spearheading it because they, the 30 percent take is seen as being too high at the moment.

And so Spotify have said they're not going to introduce ad hoc charging for audio books and podcast services and things because it doesn't make financial sense. So it is holding back consumer. Advantage with certain services as well. So the open ecosystem might actually be a vehicle for providing more services or better services to the consumer in that in that view.

Well, let's keep a track on it. I think it's something that's going to bubble over the next couple of years. And we, and we probably do need some change just, I think generally in, in all of that space, not just the Apple piece, but, but, but how big tech behaves in the world, I think is, is it's, it's a good debate to be having.

We'll keep a track on it, but let's get onto today's major subject. I am delighted to say that Nick France, [00:07:00] the CTO of Sectigo is joining us today to have a conversation about digital certificates. Nick, good to see you. Thanks for spending some time with us. Uh, join us. Want to say hello and introduce yourself and Sectigo.

So my name is Nick France, I am the, uh, the CTO and 20 something year veteran of Sectigo. Um, we are a, uh, certificate authority, so we issue these digital certificates which are used, um, all over the world and all over the internet for basically making the internet secure and

making the, your data as it travels from, you know, your web browser to whatever it is at the other end, um, and keeping it secure.

Nick, why don't we, why don't we take a step back? Why don't you describe the role that Sectego has in the interest, in the industry and what it actually does? No problem. So, uh, Sectego is, we're a certificate authority, or a CA. That's the name we give to what we do, and we create these digital certificates.

We sign them. So people come request them. They ask for them with domain names in and we sign them and create them. Um, there's [00:08:00] only a few of us that do this, right? There's a limited number of authorities because we're inherently trusted by the people like Microsoft, Google, Apple, Mozilla, Oracle, and everybody.

But to kind of step back even further, what, what do we actually do? What did digital civics do and how do they work? So. Back in, and again, back in the day, when the internet I guess was created, way before my time obviously, but, you know, there were wires connecting things, the data that was transmitted was just in plain text, it was maybe research data, whatever, anybody could pick it up, and even probably as kind of more recently as the late 90s or whatever, all of that information was still mostly plain text, and wireless started coming about, you could pick the data out of thin air and take whatever was going on, so there needed to be some kind of, We call it transport security, but you want to make sure that when you type something into it to a form on the web in your laptop here, that it's going to the right place at the other end and it's secure.

And when we say security, we really mean kind of two things. Number one, that the data is encrypted so that no one can, if they [00:09:00] can intercept it, they can't read it. But number two, that it's going to the right person, some kind of identification or authentication. So does that mean when I, when I try to go to a website?

Which doesn't happen very often, but it happens sometimes and you get a message pop up that says you're trying to make an unsecure connection. Does that mean that the certificates aren't in place or working correctly? They're either not in place or they're not installed correctly or they've expired.

Something's gone wrong with them. Yeah. And that's, I would never go to a website just like on record. I would never go to that type of website. You never click the access. I was just going to say, Dave, I don't think we need to review where you're. Unfortunately, it's a common, it's a common problem. It's not always necessarily anything bad.

It could just be a misconfiguration and that's, that's bad enough. Right. But those, those two things that we need get bound together. So we take encryption, we take a big, an encryption key. So we, I mean, we can talk about encryption, but I think most people know fundamentally how that works. We take a key for encrypting data, and then we take an identifier.

And what we [00:10:00] use is what the internet uses for identification, which is domain names. So we take a domain name, we take an encryption key, we jam it together, and that's a certificate. I think for a lot of people, though, what you're talking about, although it's the foundation of, you know, the internet, the thing that powers the world as we go, it is seen as a little bit of black magic, because when you, when you get into the world of certificate management, it's very complicated for the right reasons, because it has to be highly secure.

But a lot of people look at it and go, I don't know how it works. I'm just glad it does. Exactly. I mean, I say I do this even in customer meetings and things. It's, it's incredibly critical and

terribly unsexy. Nobody cares about it. You know, if it goes wrong, bad things happen. Really bad things happen. If it goes right, no one notices.

And I liken it to DNS domain names. No one, everybody buys domain names. But DNS is always the problem. It's terribly unsexy. You probably couldn't fill a room with like world experts on it. Um, but if it doesn't work, we're all stuck. Imagine the evening [00:11:00] event after a day of the world experts of DNS. Are you throwing a bit of IP address management?

Whacking a few. Uh, it's a bit of DNS and DHCP happy days. That is, that is, have you been to an, have you been to an ICAM conference before, by the way? . Oh, it's like, wow. . Oh, we, we have our own meetings a few times a year, so, you know, I, I know how fun those after parties can be . Well, let's talk a little bit about the actual.

process itself. So I think what we've established is the certificates is sort of the security layer that sits underneath most of what the internet does, particularly the proper sides of the internet. And they effectively ensure that you've got a secured connection. Um, but where does all of that come from?

Like, how does the process actually work? It is a bit mysterious, I think. It is. So, part of the problem with certificates, I guess, is that it's not like a traditional product that you might buy anywhere else. You buy a domain name, you can kind of go to a website, you can go to somewhere like GoDaddy, decide what name you want, give your credit card and it's yours.

That's it. [00:12:00] It's a simple process. It's kind of a transaction. Certificates, you have to do a lot of backwards and forwards, and I'm sure Rob can, you know, probably start smiling in this bit remembering, but you have to go onto the server where the certificate is, you have to type a bunch of commands to generate this key, and then generate a request, and you take that request to us, and you pop it in a form, and then you have to choose how you can prove to us that you actually own that domain name, because we're not just going to give some random person a certificate for Amazon.

com, for example. Then you get that back after this validation process, and then you've got to unpack it and go through the installation and restart your server. So it's very much a kind of a multi step process backwards and forwards between you and the person. And that is honestly how it's been done for 20 something years, but it is a manual, painful, technical process.

There's no getting around that. Presumably. If these things expire, what are the consequences for me as a website if my certificate expires? General panic, I think. Panic's [00:13:00] one. Certificate expired, yeah. Huge pop off. You get a nice big error on the website, like you said, you can't click through it. I, the, the big thing change that's happened over the past few years is the browsers used to not really care if you didn't have a certificate, they wouldn't show anything.

If you look now, even if you go to a website that most people think is innocuous, you know, let's say my mom has a blog about cats, right? A WordPress site, no one really argues that there's necessarily any need for security, but the browsers now give you a license or not secure there. And you get a little red warning next to it because they're trying to reinforce negative indicators over positive, which makes more sense.

But if a certificate expires, Starlink last year, Starlink went down for a day. I think even Elon tweeted about it and it was due to a certificate expiring. Um, I don't know if anybody's uses O2, um, in the Europe or in the UK, but a few years ago, O2 mobile went off for like a day and a half. That was an expired certificate.

Um, Microsoft regularly have outages when they forget certificates expire. I'm not blaming them. It's just they're so [00:14:00] big it happens. Office 365 goes off for a day. Why? Oh, we forgot about the certificate. So it's bad. I mean, the impact of one being forgotten about is not great. Before we come on, I'm going to come on in a minute to talk about expiry periods and because that that in in the current world is actually is changing a little bit, I think.

But when we get to that, what's the escalation process? So to say I'm owning one of those. Sites that have actually gone offline and the normal processes kind of many weeks or months of back and forth. How do you actually resolve it quickly? What's the escalation? I mean, you can, if you go back to this, to the place you got the certificate from, you can get certificates relatively quickly.

I think that's, that's one of the things that I'll talk a bit about is people may be used to this old manual process of waiting days to get a certificate. It doesn't need to be that way. The actual process can be done in. Less than five seconds when it's, when it's a bit more automated or you can even manually get a certificate in a matter of minutes and certainly doesn't need to be days.

So [00:15:00] I get the, the resolution really is to get a new certificate and it has, you have to go and get one. These things have fixed lifetimes on them, right? This is not something you can just wave your credit card and someone presses a button and it's extended a year. You have to go through that process again and get a new one.

Um, but. Dead well defined processes and they can be done in a couple of minutes. If you have the right people to run the right commands and do it right. So let's move on then and start talking a bit about some of the things that are going on specifically within your industry at the moment. Let's let's start with the time frame process.

So I believe that Google at the moment who have got a big hand in this because of, you know, their browser footprint are starting to impose a Shorter timeframes, I think that, you know, certificate validity to tell us a little bit about that and tell us the kind of the knock on impact of what's going on with that.

So there's a nice tail for the whole background of this, which I'll [00:16:00] get into. But I've been I've been with the company and doing the same, pretty much the same kind of job for 21 years now. I'm back where I started. You must love it, Nick. You must love it. I do. Well, I've not done anything else. I finished university in Manchester on a Wednesday.

I had my final exam, had an interview, started four days later, five days later, and that was 21 years ago, near as damn it. And back then we were selling certificates for 10 or 15 years. And then slowly that kind of time period has been brought down and it's gone down to 10 to 5 to 4 to 3 to 2. And then we get to 2019 and Google proposed a ballot in, we have an industry body called the CAB forum, the CA and browser forum.

So that's like us and Let's Encrypt and DigiCert. We all get together with Google and Apple and everybody three times a year and we just set guidelines for the industry. And Google brought about this ballot and said, Hey, we want to move certificates down to one year. Cause, cause like you said, Dave, they represent billions of people with every Android device, every Chrome thing.

We understand why they want to do this. They represent billions of [00:17:00] people. We want to bring it down to one year and everybody voted. And of course, most of the CAs voted no. There were two that voted yes. And one was us. Right. Didn't pass. So it didn't get the quorum of votes and, you know, Google kind of sulked and took the ball home and went.

And then we get to the The idea of them going, right, I'm off, sorry. Turn the lights on on the way out, yeah. Nothing happened, nothing happened, but it gets better. So we get to February 2020. Basically the last travel, I think anybody really did pre pandemic, we were in Bratislava for this one. And on the first day, every browser has a little half hour to talk about changes they're making.

And the guy from Apple gets up, um, and I've known him a long time as well. And he stood up and he did his thing. And then he said, Oh, by the way, we're taking certificates down to 398 days. And because Apple said it was part of their kind of policy to make any certificate work on any Apple device of which I think as of their earnings last week was two and a half billion devices, you have to do it.

You don't have a choice. You can't do something that doesn't work on Apple and does work on Google. So they went 398 days starting. [00:18:00] Like the end of the year. So everybody just went, Oh, well, where was the vote? Where? Oh, no, it was a unilateral decision by Apple. So they did that. Great. Okay. We'll, we'll get used to a year.

March last year, we had another meeting in super sunny Ottawa, where it was minus 26 without windchill. Nice. And Google said, Here's our new policy document, uh, outlining how we want this industry to move forward. And there was a bunch of stuff in there that, that's like my concern and our internal practices.

And there were two little bits of info they dropped. They said, we want to move certificates down to 90 days, and we want to move that domain verification process down to 90 days as well. You know, where you have to When you take your domain to any service, you've got to prove it's yours. Take that down to 90 days as well.

By the way, we'll have a ballot, we'll let you guys decide, and if you kids can't agree amongst yourselves, we're just going to make it policy anyway. So what's driving this? Because presumably, the knock on impacts of having to move from Yeah. issuing certificates on a Five yearly [00:19:00] basis to a three monthly basis is going to be massive and we'll come on to that in a second.

But what's driving what's driving Google's impetus here? So I mean, they've not been, they won't necessarily say exactly a list of reasons. They'll give a few ideas, but honestly, it's common sense. Shorter is better if something is bad or broken or compromised out there. The less time it's out there, the better.

So if someone accidentally issues a certificate to someone for Facebook or Amazon or Gmail, that they're not supposed to have, if that's valid for 12 months or longer, that's a 12 month abuse period, right? Someone can abuse that for 12 months. Whereas if it's only 90 days or less, By the way, we'll, we'll say 90 days isn't the end goal.

Then that's a shorter amount of time that that can be abused. And obviously Google see a lot of telemetry. They see a lot of these attacks. They see more problems than anybody else might because of their user base. And they firmly believe that it's a good idea to move down to shorter certificates. We, there's another couple of points that we can talk about later, but.

The other problem is [00:20:00] making people more agile, right? So we've had, our industry, we have had a, you know, issues over the years where we've had to cancel and get people to redo their certificates on very short notice. Um, I don't know if any of you remember the word heart bleed. It was a, an exploits in a piece of software called open SSL, which powers.

Basically everything. And I can't, I can't remember what year. I think it was 2014. I know it was my birthday. It came out on at the start of April, which was not a great day. Um, but yeah,

exactly. Woke up on the morning. It's like, what's this? I've got to deal with. And we had to go into millions of customers, millions and tell them to regenerate their certificates effectively because there was an exploit going round that could steal the private encryption key part.

And because luckily, a lot of our customers were reasonably well automated. So I had one that could click a button and do a million in an afternoon. Great. But then we find this long tail and someone goes, Oh, I've installed the certificate in an air traffic control system, you know, and after I'd [00:21:00] spat my coffee all over my laptop, I then said, Well, maybe we should figure out how to fix that.

And It took us a long time, not just us, it took everybody a long time to fix that problem. So if Google are trying to push people towards getting this all automated, so if there is another problem like Heartbleed, or I think as we'll mention, um, post quantum cryptography, uh, then when horrible things happen, you can click a button and fix it instead of going, well, uh, 12 months and this is in a nuclear power station and this is in a Power plant and they don't have time for that.

We have to fix things quick. So shorter is better is the summary really. So in the move then towards modernizing that environment and modernize that industry, what are going to be the requirements to get that in place? And how disruptive is it to move from the current situation to a more automated?

Smoother swap of certificates. Yeah, it's I mean, honestly, a lot of it depends on the maturity of the organization as with everything, right? So if you're a very, uh, mature it organization, you're a big cloud user. You'd like to automate [00:22:00] everything. You've got share fanciful puppet. You've got terraform everywhere.

It's probably easier, right? Because you've probably already got some certificates automated. You're more than likely using certificates in other places that not just your website. But if you're not, and if you're as, as it sounds like Rob may have been a few years ago, managing certificates in an Excel spreadsheet and hoping that you don't forget one of the expiry dates, then it's a big, Rob, Rob was doing it on the, uh, on an on napkins.

just said Post-it notes they were just languishing in the corner. I pick what I'm going, oh no, we, we need to deal with on . Could do, and, and you know, it was next to his password, which was stuck under his screen. Yeah, which is only six digits long. Yeah, there's a scribbled out. There's a scribbled out 20 and then a scribbled out 21 and a scribbled out 22 on the end of the password.

Well, there's ones where you turn it upside down to work out if it was a six or a nine and if you've got three months before you need to redo it. Lines, lines underneath Rob. Lines underneath the sixes and the nines. Well, that's a top tip there, Nick. That's a, that's a takeaway. Just revolutionise certificate management processes.[00:23:00]

If you're not, if you're organized and you've got some kind of automation, it's not a leap. The technologies for doing automation have been there for years, right? There's a few new ones. There's something called Acme, which anybody that's touched certificates in the past five years has probably heard of.

You can run a little client on your web server and it'll go and grab a new certificate every 30 days and you don't need to think about it. So those technologies are available, but it really, it depends on that level of maturity. I've seen. It's not an exaggeration to say I've seen, you know, top end of the fortune 500 with an excel spreadsheet and someone in the brand management team who deals with domains is handling this.

But then I've also seen organizations who are cycling certificates every seven days and don't even think about it. So I think the recommendation, I think the recommendation. for organizations listening to this is actually get your arms around it. Ensure that there's a process in place and then, and then look at tooling because actually what you were doing once every six years, whether you like it or not, is that's about to fundamentally change.

There's a customer organization, you know, you need to be aware of that stuff. [00:24:00] Yeah, it's going to be six times a year to start with. And just to be clear as well, Google's 90 day thing, it's not the end goal. They'll incent, they incentivize me today to give someone a certificate for 10 days. I have, I have technical incentives to give you a cert for 10 days today, so 90 days isn't the end goal.

I don't think it's going to go down as low as 3, 2, 1. I think 7 to 10 is going to be the sweet spot. Um, for various reasons, but it's the end goal is shorter, but yet order of magnitude different. And therefore, how you manage these things needs to be sort of deeply considered. And then maybe we can bring our conversation today to a bit of a conclusion by actually.

Looking forward into the world that you mentioned earlier, Nick. So a world of post quantum, we all know the impact. I think that quantum is going to have on things like encryption. So presumably getting fit for this sort of stuff and the sort of pressure Google's putting on has got its eye on that problem, right?

Yes, I mean that's that's I think that's one of the reasons I think they're reasonably open about that being one of the reasons [00:25:00] if you've got billions of certs out there, and they're all reliant on one of two crypto things, something called RSA and something called ECC. They're both mathematical things that rely on stuff that's hard for current computers to do.

And quantum computers, in theory, when they arrive and they're powerful enough, they're going to be able to do, basically break that encryption, try every single key in orders of magnitude, something that would take till the heat death of the universe could be done in a Wednesday afternoon. Right. Right.

And so, that's bad for everybody. And because we need to get people prepared for that kind of change, if they look at things like certificate management, certificate life cycle management tools, Not only do they have the peace of mind, everything's all sorted, I don't need to worry about these expiries.

When some researchers in China tomorrow come out with a, Oh, we've got a quantum computer by the way. They go, okay, well, here's the new types of certificate. It might take a few weeks or whatever for that to come out. Click a button. They're, they're, they're happy. They're safe. Everything's cycled through.

Everything's automatic. So that post quantum thing, it's, it's gonna hurt our [00:26:00] industry, which hurts the internet. But if everybody's prepared to just be able to click a button and cycle through it, then we'd be in a really good place. But that's, that's been my job for a few years and will be my job for the next couple of years to try and get people to get to that level of management so that whether it's post quantum, whether it's Heartbleed 2, whether it's a silly mistake by some other CA, we want everybody to be able to click a button and have these things cycled through and not worry about them.

Do you feel that there's wide enough understanding and acknowledgement of the changes that are going on here, because they're quite significant, aren't they? Especially when you

think about the sort of, um, end user organizations we talked about a minute ago, which have got, you know, processes that may well have been in place for, you know, 10 years that are, that are going to significantly have to change.

And it is one of those things. in an organization that certificates are taken sort of deeply seriously. Yeah. Um, and the risk, the risk around getting them wrong is, is very, very high. You could lock all your users out. [00:27:00] You could lock a website. You could do many, many different things. So do you think the need to change is well enough understood across the industry at the moment?

Honestly, no, I don't think it is yet. I think education about these changes is it's not there yet. I mean, we're trying to do it. We're trying to do a lot. I've been on countless, you know, webinars and things and customer meetings and, you know, great podcast like this to get the word out. But I think the problem is, as far as I can see it, is while we can all shout about it in the industry, one thing Google didn't give us is a date.

Right. They haven't said this is when this is going to happen and what we're finding. Unfortunately, as you go to an organization, you get the right person. You say this is coming. They understand the gravity and they go, I'm not going to bother until I know when I have to do it, which is poor planning. But I mean, when is when a big organizations not always been really forward planning a lot of these things, especially this unsexy, you know, yeah.

Oft misunderstood technology. So I think once we get a date on this, even if it's a, [00:28:00] it'll be, we'll get 12 to 18 months notice, right? And on Google, don't do this thing and say it's tomorrow. So when we get that date, I think the pressure will increase. I think the marketing and the knowledge and the educational increase, and hopefully that'll get people more motivated to do it because if they don't.

I mean, it's the first 90 days after the deadline is going to be, I wish I could take three months off, but I don't think that's going to be a possibility. It's an interesting example of the power of a big tech company where they can just say it like Apple did, like Google are doing and they, everybody says, Oh, we've.

Probably have to do it, but it does say like it's, it feels a little bit like maybe the tail wagging the dog considering you had a consortium who would vote on this stuff and it would be a considered thing and then they just railroad straight through the center of it and it's, you know, it's big tech power again, you know, and you, you argue that, okay, it's the right thing to do, but the impact.

of what they're doing to so many organizations you discussed is quite high. And so it's going to [00:29:00] drive a lot of cost in organizations to be able to get this sorted out. And I think, um, although technically it's a good thing, it may not be, the approach to it may not be the best. I think a lot of people have said that to me.

I mean, a lot of this, there's always talk with like the EU CAs and maybe EU customers. Can we, can we do something with the EU? Can we drive some antitrusting? Can we make Google not do this? And you're right, Rob. I, I, and I get it because it is ultimately a good thing for everybody. It's, it's, it's very hard to argue against.

Then trying to do a good thing, even if perhaps the approach isn't great. But at the same time, it's been 12 months since they announced it. They haven't given us a date if I'm forced to guess on a day, I would like to see some proposal come out this summer with maybe a 12 to 18 month effective date. So you're looking towards the back end of 25 and between the announcement from 2022.

I mean, that's a good 33 and a bit years. It's A reasonable amount of time for someone to start making these changes. So yeah, I see. It is a [00:30:00] bit of a problem that the way they perhaps approached it, but there's honestly good reason they've done it that way because they wouldn't get us to all agree anyway.

So well, I think it is moving forward and given the world is changing and cyber gets ever more challenging with some very big steps coming up. I think it probably is the right thing to do, but it also requires Planning and consideration and given it's the end of 25, that means it should be in organization planning for 2024 to make sure you're not running long.

So I guess, um, to wrap up, Nick, say you're advising Rob of 15 years ago. He's got his He's got, he's got his sticky, sticky notes, post it notes system in place to manage his certificate. It was perfect. Dave, I'll tell you, it was the best system ever built by humankind. And his napkins next to him. Exactly, pile of napkins.

Uh, he's, he's going into triple digits on his increment on his password at the end. Um, what advice would you give Nick to an organization that need to modernize? Maybe [00:31:00] not to that extent, but you know, need to modernize into, into what you've been describing. Yeah, I mean, the first step we've been advising people is is to look at the automation solutions.

And that starts, honestly, with a lot of the tooling, whether it's something from us, whether it's these third party management tools that are available, get get a handle on what you have. So do there's something called certificate discovery where you can go right. I don't know what certificates I've got, let's get them all discovered.

Cause once, once you have them all discovered, even if you are, and I'm not going to advocate this, but I've heard people say it, okay, I've got to do this six times a year, I'm just going to find an intern, or I'm just going to offshore some guy that's going to click this six times a year. I don't like it.

And some people are going to do it, but if you're going to do it, let's get. At least a handle on what you have. So go, go speak to whether it's your CA, your, your MSP, your vendor, get, get some tooling together, get the discovery together, find the certificates you have, and at least have an understanding of what you've got and whether you can start to automate it.

I don't expect everybody to go a hundred percent and [00:32:00] be able to click a button and never think about it again. But as you've said, or we've all said, really the impact this can have, if it goes wrong, when it goes wrong is huge. So you need to be in some kind of position where you understand you.

certificates. You at least are starting to think about doing some kind of management and automation, even if it's going to take 12 months, but just start to get a handle on it and start to look at it today. Even though I can't give people a date as to when this is going to happen.

What you've been looking at this week, Sjoukje?

So each week I do some research on related ideas in transformation and tech. And this week I thought we should take a look at some cybersecurity trends to watch for in 2024. So in 2024, the field of cybersecurity will experience significant changes driven by advanced AI tools and social engineering tactics.

So AI will play a huge role in cybersecurity, enabling automated, responsive, [00:33:00] predictive analytics, and improved threat detection. Election years will continue to be prime targets for this information campaigns and social engineering attacks and ransom attacks will escalate as well. So a question to all of you, do you think that these are the biggest

strengths In cyber security this year so that the whole fake news agendas rising fast and now, uh, nation states are looking about how they tackle it.

I would add, though, there was this fear that you can just create a video of a politician saying something that would corrupt an election result. However. Globally, if you look at the performance of most politicians, they don't need any artificial help to mess up the situation. Um, they're in or say something stupid.

So, I mean, there's balance there, but yeah, there is this thing about, um, where does it go next? But there is this fear about human manipulation through technology that affects a very dramatic outcome. I think for me, it's the, the, that's a symptom of the [00:34:00] sophistication of, of attacks these days, where the, you know, attack still happened.

In a very techie way, kind of underneath the waterline, or they might happen virally. But yeah, the, the, the social attack that you're describing, which let's face it, unfortunately has been with us for the last couple of election cycles at this point. And depending on where your views lie, you can see impacts or not of, of that.

But yeah, I think getting that in hand somehow. Which is a very different way to think about cyber warfare, isn't it? It requires very different mitigations. It's that thing about, uh, one of the biggest investments is now about detecting AI, and I think Facebook Meta said they would now start to tag AI content automatically, so as it's uploaded, it's detected, and people can become aware.

So, uh, there is that. How many circular loops are there do you think in between creating AI content, then having it detected, then using an AI to stop the [00:35:00] AI detecting the AI? It's an arms race, isn't it? It's a technology arms race. It's a cat and mouse game, yeah. It's a lot of content. Did you see the article the other day?

Sorry, but the um, the fake video and the stuff now is scary. There was some Hong Kong company, the guy got scammed out of 25 million dollars because they had AI video of his like executives or their executives saying you need to transfer this money to these accounts and they went and did it. So I mean the election misinformation is a big one but they're already using AI video to scam people out of millions of dollars and I, I, it scares me that it's that accurate.

So soon comparatively, right? I mean, we've seen phishing emails, we've seen voice stuff, but when you can replicate someone's video with the right speech and the intonation and stuff, it's, I mean, how do you fight against that? It's incredibly difficult. It is amazing. It's one of the things that I say sometimes when people talk about AI and they go, well, you know, AI, it's just like robots and factories, isn't it?

You know, it's like, it's only going to have an impact, but it's like, is it, is it? Really like that. I think there are [00:36:00] some very marked differences here in the one you point out there, Nick, I think is. Right at the heart of that, the level of ability to very quickly fool another human being, it's way past the Turing test at this point.

You can't trust what you see and hear anymore, which, whether it's disinformation or whether it's someone trying to say, hey, can you quickly wire me a few grand? I mean, I don't know, how do you, how do you not get along with not being able to trust what you see and hear? There was a cracking, uh, article about a scam that went to a mother from the son saying I'm stuck in this foreign country.

Send me the money. And the scammer got back this massive tidal wave of this mother giving the, uh, I can't believe you've got to this position in your life. Why can't you sort out your

finances? I'm not sending you money. You need to get yourself out of it. You picked the wrong mother to mess with. You picked the wrong mother to mess with on the scam.

So I'm curious, Nick, is AI also going to impact the certification industry? Yeah. I think it is a little bit. Yeah, because I mean, we, we talk [00:37:00] primarily about the search that we deal with. You talk about websites and web services and stuff, but there's a bunch of other different certificate types and some of them, especially in the EU, there's something called the EIDAS where you can actually get a certificate.

It's the same as we talked about, but it's issued to a person. And, you know, in many European countries, you can use them to do, you know, tax returns or interaction with the government and, and they have to be strongly identified. Right. So you can do some of the verification through things like video chat.

Well, how can we carry on doing that? If the video chat can be just as easily faked, it's. It's, it's a difficult challenge. So we're end up, you know, having to go back to where you do face to face verification for things. Um, so yeah, it absolutely will have an impact because fundamentally everything we do is based on verification of someone's identity.

And it's fine if it's a DNS name, but if it's people and if it's companies and it's, you know, organizations and individuals, that's way harder when there's technology out there that can just forge it with a few button clicks. Right. Well, look, Nick, thank you for spending some time with us this morning and helping us through understanding, um, not only [00:38:00] the sort of criticality of the certificate infrastructures, but actually the, uh, the, the changes that are to come and how we respond to it.

It's good to see you. Thanks very much for having me. It's been great. Thank you. Now we end every episode of this podcast by asking our guests what they're excited about doing next, and that could be it's half term next, and I'm taking some time off with the kids, or it could be something exciting in your professional life.

So Nick, what are you excited about doing next? It's almost a half term. I mean, professionally, honestly, it's just the next few years are going to be the biggest change I've seen in 20 years, so I honestly am looking forward to it. But personally, the big thing, I have two kids, and their birthdays are in March, very close together.

Not this weekend. Next weekend, some synchronization going on there. Six days apart. You know, we timed that pretty well. You know what? My kid's one was born the 11th one on the 18th. It makes for a birthday parties. I'll tell you that, isn't it? But we've got a bit of a weekend with my, my eight year old son.

So we've got on. Next Saturday morning, we've got a show in Manchester called Bricktastic, which is like a [00:39:00] Lego show. So it's a big exhibition. I've been to Bricktastic. It's fantastic. It is fantastic. My retired Lego fanatic dad's coming with us this time. Saturday afternoon, he wants to make his own big dinner for me and my wife and his sister, which I love cooking.

I'd happily not do any of this tech stuff and cook. So we're doing like sushi and Japanese fried chicken and all that. And then Sunday morning, we're going back to Manchester to the arena for a monster truck show. Right. Proper American monster trucks. So next weekend is the highlights of my, can you adopt me please?

That sounds like a best birthday party ever, doesn't it? Just monster trucks. Exactly. Properly. And we did, we did it last year. I think the monster trucks and it's, I've never seen anything like it. And in an enclosed arena, it's, it's deafening, but fantastic. So very much. Enjoy that.

What, who does the, when you make the sushi, who makes the rice and who does the actual sushi construction?

Um, I do the, I do the rice and he, he honestly does, I've got, we had to film it for a kind of a school project, which sounds [00:40:00] daft, but he's there with the, you know, rolling the stuff in it and cutting it up and things, he's, he loves it, he's taking after his dad when it comes to cooking, which I like, so we're happy and looking forward to a good meal on Saturday.

Well, have a wonderful time. Thank you. So a huge thanks to our guests this week. Nick, thank you so much for being on the show. Thanks to our high quality producer Marcel, our sound and editing wizards, Ben and Louis, and of course, to all of our listeners.

We're on LinkedIn and X, Dave Chapman, Rob Kernahan, and Sjoukje Zaal. Feel free to follow or connect with us and please get in touch if you have any comments or ideas for the show. And of course, if you haven't already done that, rate and subscribe to our podcast.

See you in another reality next week [00:41:00].

About Capgemini

Capgemini is a global business and technology transformation partner, helping organizations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 340,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from strategy and design to engineering, all fueled by its market leading capabilities in AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2023 global revenues of €22.5 billion.

Get the future you want | www.capgemini.com

Capgemini