Audio file

Securing the Modern Vehicle Episode 2.mp3

Transcript

00:00:01 Speaker 2

You are listening to the HCL engineering and R&D Services Podcast powered by CTO Straight Talk.

00:00:08 Speaker 3

Welcome everyone and thank you for joining us today for our second in a series of podcasts on securing the modern vehicle.

00:00:15 Speaker 3

This series brings together engaging conversations with cyber security thought leaders from HCL technologies and Cybellum as we look at the evolving industry challenges, discuss some of the latest cyber security.

00:00:30 Speaker 3

And share insights to stay ahead of emerging cyber threats that are faced by the automotive industry.

00:00:37 Speaker 3

In the last episode we had an exchange on the rising threats and automotive and how a vehicle can be attacked not only onboard the vehicle but also from a remote location off board.

00:00:50 Speaker 3

The range of types of breaches was also discussed with outcomes ranging from personal data theft.

00:00:58 Speaker 3

Or ransomware.

00:01:00 Speaker 3

Or even as severe as hijacking the control of features or functions within the vehicle while it is being used by the driver.

00:01:09 Speaker 3

And the conversation led to the question around what actions are being taken across the industry to secure the vehicle.

00:01:16 Speaker 3

Which leads us to today's topic.

00:01:18 Speaker 3

ERA of regulations.

00:01:21 Speaker 3

Hello and welcome.

00:01:23 Speaker 3

I am Chris Berman, the vice President of strategic initiatives and the Transportation division at HCL Technologies, and I am excited to be the moderator for today's session.

00:01:34 Speaker 3

I'm being joined by two esteemed experts in cyber security.

00:01:39 Speaker 3

Neal Berkowitz is the founder of Echo Consulting and formally a manager and vehicle cybersecurity at Fiat Chrysler Automobiles, now still Lantis

00:01:49 Speaker 3

And we are also joined by Altra tell who is the Vice President of Strategic alliances at side, Belum.

00:01:57 Speaker 3

Today's episode will focus on the area of cyber security regulations being implemented in the automotive industry and we are privileged and excited to have Neil and I'll with us.

00:02:08 Speaker 3

Gentlemen, thank you for joining me today.

00:02:11 Speaker 3

Could you please provide a deeper introduction about yourself in your background for the audience?

00:02:16 Speaker 3

And IL perhaps you can get us.

00:02:19 Speaker 4

Sure, thanks Chris and happy to be here with you and Neil.

00:02:23 Speaker 4

So my name is Al.

00:02:25 Speaker 4

Try tell I'm I I have more than 20 years of experience in enterprise software.

00:02:31 Speaker 4

Worked in small startups as well as Motorola and IBM in various roles anywhere from Level 3 support pre and post sales consulting, product marketing and product management.

00:02:43 Speaker 4

I joined cerebellum in 2019 and today I'm responsible for our relationship with LG Vehicle solutions and our various collaborations with with LG as well as other activities we have with customers around cyber security and regulatory requirements.

00:03:02 Speaker 3

Thanks I'll.

00:03:04 Speaker 3

We'll can you share with us your.

00:03:05 Speaker 5

Background sure good morning Chris.

00:03:10 Speaker 5

My name is Neil Berkowitz and I started my company Echo Consulting after I left FCA, which as you mentioned is now still antis in 2018. And while I was at FCA I started the vehicle Cyber Security Group there.

00:03:27 Speaker 5

Prior to that FCA, I worked in the design and development of electronic hardware, software and vehicle system.

00:03:37 Speaker 5

I also have a background in both industrial and military electronics and I enjoy bringing all of that experience with me to my consulting company, and so I do a lot of different things with ECHO consulting in those areas.

00:03:55 Speaker 5

For a a variety of customers.

00:03:58 Speaker 5

Thank you.

00:04:01 Speaker 3

Thanks Neil and I'll.

00:04:03 Speaker 3

So first question I have for both of you, given all your experience, it seems that until recently.

00:04:10 Speaker 3

There have not been any regulations around cyber security in the automotive industry.

00:04:14 Speaker 3

A lot of collaboration between groups.

00:04:16 Speaker 3

Some policies that have been written, but we now see that there's a change in this situation and there are regulations that are coming to the forefront.

00:04:26 Speaker 3

Uhm, what?

00:04:28 Speaker 3

What changed to the situation that this is happening and who's affected by it?

00:04:33 Speaker 5

IL, you want to take that one first.

00:04:35 Speaker 4

Yeah, sure.

00:04:36 Speaker 4

So previously I think manufacturers have been working on cybersecurity already for quite some time, in some cases more than 10 years ago, but things have not been standardized, which means that different manufacturers had, you know, each manufacturer had their own standard.

00:04:56 Speaker 4

But UM, some OEM's were doing some activities expecting Tier 1 suppliers to do the rest. You know there was no standard methodologies of of of doing sub security activities and I think where the regulation is changing in last.

00:05:16 Speaker 4

Definitely in the last two years, uh or so, with the WP 29, the UN R155 and R156 in the eyes of 21434 is that?

00:05:27 Speaker 4

Vendors in both sides of the equation, both OEM and tier Tier 1 and Tier 2 suppliers are.

00:05:34 Speaker 4

Accelerating their cybersecurity activities and align to the same terminology, same methodologies, and and and both ends are working towards the same.

00:05:47 Speaker 4

The same mean, same end.

00:05:53 Speaker 5

OK, I I guess I'd like to add to that that you know prior to WP 29 there were a lot of best practices put out by various organizations.

00:06:02 Speaker 5

Friends and those organizations had no legal standing, so it was a best practice only.

00:06:11 Speaker 5

And if you wanted to follow it you could and you could take pieces of it.

00:06:15 Speaker 5

Or you could do the entire document, but now that WP 29 is in place and it is a legal standard.

00:06:22 Speaker 5

If you don't meet it, you won't be able to sell cars.

00:06:26 Speaker 5

In the regions affected by that and, we should point out that right now WP 29 is not a global standard, but it is a standard that applies to primarily Europe and multiple Asian countries, not necessarily the US. At this time. A lot of pundits.

00:06:45 Speaker 5

In the field had said that people weren't doing enough.

00:06:49 Speaker 5

And I think the various regulatory agencies have taken that those statements to heart, and so OEMs, at least from an outward perspective, have shown a lot more activity to the public and what they're doing is, you know, trying to fix.

00:07:09 Speaker 5

Any issues that they may have had with respect to some of the best practices I I also think that that everyone is still doing their own thing in terms of security.

00:07:23 Speaker 5

And the paths there may be quite different from one organization to the next, and an example I'd give of that would be the many organizations we're only worried about telematics controllers early on in this process, and since that time, everybody.

00:07:44 Speaker 5

Now I believe recognizes that you have to look at the vehicle as a whole, and there's lots of attacks services to go after.

00:07:52 Speaker 5

The problem for governments was is that.

00:07:55 Speaker 5

They really couldn't tell what everybody was doing.

00:07:58 Speaker 5

So if you start applying regulations you start establishing.

00:08:02 Speaker 5

I guess what I'd look at is minimum levels of compliance to some sort of cyber security standards.

00:08:12 Speaker 3

So that that's really interesting that it's looking to now have some form of a minimal standardization. And can you share with us a little bit more about what is within this WP 29 regulation?

00:08:27 Speaker 3

What would it take to comply?

00:08:29 Speaker 3

What are some of the?

00:08:30 Speaker 3

The key best practices around it, and when does?

00:08:34 Speaker 3

It go into effect.

00:08:38 Speaker 4

So it's.

00:08:38 Speaker 5

OK, go ahead.

00:08:41 Speaker 4

Uhm, from from you know when people ask me about WP 29, I typically refer to a paragraph 7.2 which is kind of the heart of the regulation and it talks about the different processes that you should have.

00:08:56 Speaker 4

Uhm, in order to perform cyber security activities.

00:09:01 Speaker 4

And if you look at that list, it it pretty much the way I can summarize it.

00:09:05 Speaker 4

I summarize it to myself.

00:09:07 Speaker 4

Is it covers the entire range of activities you should have in a in an organization, anywhere from awareness to cyber security down to having all the processes to assess the risk, the vulnerabilities that come with it.

00:09:20 Speaker 4

Continuously monitoring.

00:09:22 Speaker 4

For new threats and so on.

00:09:24 Speaker 4

So it's pretty.

00:09:26 Speaker 4

Comprehensive, uh yet it is not, UM, providing the the lower level details of exactly how you should do the activities and what.

00:09:36 Speaker 4

What are the deliverables you should have to the smallest level of details?

00:09:42 Speaker 4

This is where the ISO two and fourth before comes to play.

00:09:45 Speaker 4

There is one.

00:09:48 Speaker 4

One list that is technical is the annex five of the regulation, which talks about the threats and mitigations you should cover at the minimum, and this is a, uh, providing very technical details on on what what you should look at.

00:10:06 Speaker 5

Specifically, with regard to the timing, Chris WP 29 applies to any new vehicle that OEM would launch that they must comply by July of 2022 and then for existing vehicles they have until July of 2024.

00:10:26 Speaker 5

To meet the regulation.

00:10:27 Speaker 5

I also want to add that I'm not so sure that ECUNYC is trying to standardize as much as they want to establish what we just mentioned. The minimum level of compliance. And like I said, the each company cybersecurity journey is different.

00:10:47 Speaker 5

They come from different backgrounds and their view of cyber security may differ from one to the next in in in quite a large range.

00:10:57 Speaker 5

Early on there were many OEMs that didn't even.

00:11:00 Speaker 5

I think this was an issue that you could fix this problem by not letting people in through the telematics unit, and they've now realized that that's not really possible just to stop the threat there.

00:11:14 Speaker 5

If that were true, all your retail and banking institutions would never be hacked, so.

00:11:20 Speaker 5

I think they've they've become more accustomed to the idea that the whole vehicle must be looked at it.

00:11:28 Speaker 5

It's in in his y'all said it, it's more about the what, not the how they don't get overly prescriptive in how to implement something.

00:11:38 Speaker 5

Uh, and uh again. There are two parts to it. The 1:55 and 156. The 1:55 deals with process and 156 really deals with a software update management system or sums as it's abbreviated. So both of those parts have to be met in order to meet the.

00:12:02 Speaker 3

Thanks for that overview and in with that discussion, and I owe you talked about 21434.

00:12:10 Speaker 3

And we've been spending some time on WP29. Is there any relationship between those in ISO 26262 and Neil? Maybe you can start us.

00:12:23 Speaker 5

Well, 26262 wants to make sure the car is safe. So if a part wears out or breaks a, that's a safety issue under consideration.

00:12:34 Speaker 5

It also could be a software defect that causes a controller to misbehave and and that is a likely single event, for instance.

00:12:44 Speaker 5

The difference with cyber security is that an attacker who wants to go after a vehicle wants to make something happen and they have the ability to string together multiple events with some certainty that they will occur once they figure out how to achieve them.

00:13:03 Speaker 5

And that's not a.

00:13:04 Speaker 5

Natural or random fault, whereas in 26262 it's more of a random situation where yeah we could have this happen, but then you have to look at what else has to happen to have a true safety situation now in cyber security attacks to date.

00:13:24 Speaker 5

Have involved multiple steps and I like to call those steps pivots and for example some of the more recently publicized attacks have involved.

00:13:35 Speaker 5

6 to 7 pivots, and with those 6 to 7 pivots your wind up with a situation. If you're looking at it from a 26262.

00:13:45 Speaker 5

Perspective, that's unlikely.

00:13:47 Speaker 5

The probability of six or seven things going wrong is highly unlikely, so I see that as the main difference between.

00:13:55 Speaker 5

The safety.

00:13:58 Speaker 5

26262 document and either 21434 WP 29 that's the primary difference.

00:14:05 Speaker 4

I like to take a look.

00:14:07 Speaker 4

At the different if it it from a different angle, which is that if you the issue of static versus dynamic.

00:14:15 Speaker 4

So if you take for example the breaking system, if you design and develop and test it to to perform safely under different.

00:14:25 Speaker 4

Road conditions such as humidity, uh, you know, temperature, speed and so on.

00:14:30 Speaker 4

On once you finish all the testing that's required and and then the 26262 is is not one that's easy to pass.

00:14:39 Speaker 4

Uh, but once you go through all these rigorous testing, you're you're basically done, and those brakes will be considered a done deal, ready to ready to go on the road.

00:14:51 Speaker 4

Unfortunately, software doesn't work that way.

00:14:54 Speaker 4

Uh, just uhm.

00:14:57 Speaker 4

Around 18,000 vulnerabilities are discovered each year and the numbers go up and up. So if you finished your cyber security testing for a certain product today and this will be considered safe and secure today. Unfortunately tomorrow there could be new vulnerabilities discovered and this happens.

00:15:18 Speaker 4

All the time.

00:15:19 Speaker 4

And that product is a risk.

00:15:22 Speaker 4

Risk poster is actually not as good as it as it is today, so that requires continuous monitoring for this new safety risk called cyber security.

00:15:36 Speaker 4

Uhm, and it's not enough anymore to just finish your testing and you're done. So the the WP 29 and.

00:15:43 Speaker 4

The eyes will talk.

00:15:44 Speaker 4

A lot about.

00:15:45 Speaker 4

Monitoring and I know some some manufacturers. From what I've heard, we're not so keen to perform continuous monitoring for issues, but this is unfortunately the norm today. Uh, nevertheless both the WP 29 and.

00:15:59 Speaker 4

The ISO don't talk.

00:16:01 Speaker 4

They don't enforce a specific frequency.

00:16:04 Speaker 4

Of monitoring.

00:16:06 Speaker 4

Uh, so it will be interesting to see what, uh, what it will entail in the future.

00:16:12 Speaker 4

For from.

00:16:16 Speaker 3

So I oh that's interesting.

00:16:17 Speaker 3

You know you talked about frequency is something that you know is going to be part of a changing dynamic, and how automotive manufacturers.

00:16:25 Speaker 3

Have to look at.

00:16:27 Speaker 3

Uhm, protection against cyber security?

00:16:30 Speaker 3

Are there other elements of this regulation coming into effect?

00:16:35 Speaker 3

That's going to change some of the practices within not only an OEM, but even with their supplier partners and how they have to look at the business that they do.

00:16:45 Speaker 3

Can you comment on that?

00:16:48 Speaker 4

So, at least from what we've seen in Sebelum, is that there were some Williams that try to delegate the activities in their entire T2 to suppliers, expecting them to do all the testing saying this is not our software you should do.

00:17:07 Speaker 4

All the work.

00:17:08 Speaker 4

And just report back to us in some other cases OEMs have been more proactively testing on their own.

00:17:18 Speaker 4

And I think the situation is changing in the both ends.

00:17:20 Speaker 4

Uh, OEMs realize that they cannot fully trust US suppliers on on their end, and they.

00:17:26 Speaker 4

Got to test both the.

00:17:27 Speaker 4

Products, uh independently and also their interconnections and how they operate.

00:17:34 Speaker 4

Uhm, how they interact with each other right in the vehicle as a whole.

00:17:39 Speaker 4

And on the other end, suppliers have stepped up quite a lot there.

00:17:43 Speaker 4

Cyber Security Act and we see that all around in different manufacturers and they're doing a lot more testing and today.

00:17:52 Speaker 4

Hey, uh, also they have to go through audits, bio NS and also by regulation bodies so they they also perform a lot more activities than they used to.

00:18:06 Speaker 4

At least from what we see.

00:18:09 Speaker 5

Yeah, I think the regulation is definitely going to force people to do things differently and with respect to the relationship between OEMs and suppliers.

00:18:20 Speaker 5

That has changed.

00:18:21 Speaker 5

Dramatically with just the advent of cyber security requirements because different OEMs have different requirements, modules that used to be more or less a commodity module have no longer become a commodity from the standpoint that.

00:18:40 Speaker 5

If they are applying different instruments in order to get the module safe and one supply one OEM has one set of requirements and another one has a different set.

00:18:55 Speaker 5

A big challenge for the supplier is going to be how do I meet both sets of requirements with one module that used to be a commodity that also goes back to the OEM and that they are not going to be able to take advantage of scale.

00:19:11 Speaker 5

If they used to buy something as a commodity and it's something not something that makes their car.

00:19:17 Speaker 5

Differentiated from another, that'll be a cost disadvantage if those modules can't become a commodity from a cyber security standpoint at some point in the future.

00:19:30 Speaker 3

So Neal a question I would ask for you given your background coming from many years in in at an automotive OEM.

00:19:39 Speaker 3

Do you think at some point this will become part of it?

00:19:44 Speaker 3

It's part of the process is that automotive manufacturers have like wood.

00:19:48 Speaker 3

Cyber security or proving out?

00:19:51 Speaker 3

You know that there are no vulnerabilities become part of a peep app process or a PQP.

00:19:57 Speaker 3

Or how do you see that evolving with time?

00:20:00 Speaker 3

Will it become more formalized or will it continue along the path that it's been following?

00:20:06 Speaker 5

Yeah, I I.

00:20:07 Speaker 5

Absolutely believe that this will become part of the pepap process at any supplier that has that or a similar method for qualifying the vehicle.

00:20:18 Speaker 5

You can't get that far down the road and go back and redo everything, so in order to make sure you know this is going to have to be.

00:20:27 Speaker 5

Planned for.

00:20:28 Speaker 5

Uh, and earlier we've touched on the 21434 IL brought up and 21434, even though it is more prescriptive than the the WP 29 Regulation, different OEMs are going to get still be able to.

00:20:48 Speaker 5

Approach that differently, but uh, when they start looking at how do they meld all these different features into a product they're going to have to do that on some kind of schedule, and the people app is the obvious way to do it.

00:21:05 Speaker 5

I also think that WP 29 is a good start because as I would call it, it's kind of a a mom and apple pie approach.

00:21:13 Speaker 5

It's going to get people moving and moving without having to all of a sudden put tremendous restrictions on what they can or can't do in a module.

00:21:23 Speaker 5

But by getting everybody moving and getting everybody moving in One Direction.

00:21:28 Speaker 5

I think the you know the uniformity of that in the end will be benefit to the industry because I'm not sure anybody can sell cars based on.

00:21:37 Speaker 5

I have a better approach to cybersecurity.

00:21:41 Speaker 5

Some may try.

00:21:42 Speaker 5

I, but hackers can have a way of humbling you pretty quickly in that regard.

00:21:49 Speaker 5

I am looking forward to having other standards which would be more comprehensive and I think that can happen someday because if you look at, uh, can.

00:21:59 Speaker 5

For instance, they can messaging system vehicles would not be as advanced today if that hadn't come along as a standard, and I think that that will.

00:22:09 Speaker 5

Also be true with cyber security if we can arrive at some standards that everybody can agree with, it would benefit the industry.

00:22:17 Speaker 5

On the whole.

00:22:20 Speaker 3

Shoots O'Neill based on your comments.

00:22:22 Speaker 3

One of the things that makes me think about you know we've been talking about really kind of what's been in the past, the.

00:22:30 Speaker 3

More mainstream approach to how the car is developed and processes around that.

00:22:35 Speaker 3

But the cars evolving is, well, we're we're starting to see operating systems in in vehicle infotainment systems like the Android operating system and through that it enables people to do more apps and apps that may be specific to a vehicle on part of an App Store for.

00:22:53 Speaker 3

How should the?

00:22:54 Speaker 3

Auto industry think about those apps and security around those apps and I all given your background in cybersecurity.

00:23:02 Speaker 3

Maybe you can give us some insights how to think about that.

00:23:06 Speaker 3

As the industries evolving.

00:23:09 Speaker 4

So I think, uh, what I see at least manufacturing are doing.

00:23:14 Speaker 4

Obviously as bomb is becoming a big topic in the industry and.

00:23:19 Speaker 4

Uh, and having a complete as bomb of components meaning.

00:23:23 Speaker 4

Uh, that a manufacturer needs to have a complete inventory of his.

00:23:28 Speaker 4

Configuration, including all the third party apps and software libraries, and.

00:23:34 Speaker 4

What have you?

00:23:35 Speaker 4

Uh, that needs to go into into components and cybersecurity activities should cover everything.

00:23:42 Speaker 4

Uh, including the third party.

00:23:46 Speaker 4

Apps and maybe just to point to Neil previous comment on standard standardized cyber security in the future.

00:23:54 Speaker 4

Maybe related to husband is the first hint.

00:23:57 Speaker 4

Is that as bomb has been very, uh.

00:24:02 Speaker 4

It was highly differentiated across in what does it mean and what should it include was not standardized, and we see first signs of standards like aspx and cyclone.

00:24:14 Speaker 4

The access is is a standard way for the industry to cover as bombs, and this.

00:24:19 Speaker 4

This should definitely.

00:24:22 Speaker 4

Means that cybersecurity, like vulnerability information and so on would also get to that level in the future.

00:24:32 Speaker 3

Thanks Al and I would say this has been a just a fascinating exchange and very insightful.

00:24:40 Speaker 3

You know, and one you know, take away from me from this is that it's apparent that there isn't necessarily a destination state that we're gonna reach where you've achieved absolute security on a vehicle you know you've.

00:24:53 Speaker 3

Talked about how software is dynamic and it's going to be ever changing, which means that.

00:24:58 Speaker 3

Even with the pending regulations that are coming in like WP 29, there will have to be evolving measures and methods in order to stay ahead of the threats that are out there.

00:25:09 Speaker 3

And so I'd.

00:25:10 Speaker 3

I'd like to thank both of you for sharing your insights today.

00:25:15 Speaker 3

I think it's given us a lot to think about with respect to how policies and regulations are influencing the industry and where we are on the journey of cyber security and securing the vehicle.

00:25:29 Speaker 3

Come to our audience.

00:25:30 Speaker 3

I would like to say, you know, perhaps a conclusion that you've drawn is that even with the regulations that are coming with cybersecurity protections, there has to be a continuous change and evolution to stay ahead of any threats.

00:25:45 Speaker 3

So as a result, the industry must be strategic in continually designing and implementing new or even more advanced features to ensure that the vehicle is secure.

00:25:55 Speaker 3

So I would like to invite the audience to join us at our next session where we will have two new industry experts join us that will delve deeper into the topic around the evolving automotive cyber security strategies and how to keep the vehicle secure.

00:26:11 Speaker 3

Until then, I wish you all the best.

00:26:15 Speaker 3

Thank you.

00:26:16 Speaker 4

Thanks, thank you, Chris.

00:26:16 Speaker 5

Thank you Chris.

00:26:18 Speaker 4

Thank you Neal.