PORTUGAL WEBSITE NOTICE

17 de novembro de 2026

AVISO DE VIOLAÇÃO DE DADOS PESSOAIS

O QUE ACONTECEU?

A 25 de julho de 2026, a WireCo World Group Inc. e as suas subsidiárias («WireCo» ou «nós») detetaram atividade não autorizada nos seus sistemas informáticos internos, que posteriormente se revelou ser um ciberataque levado a cabo por um agente malicioso conhecido e sofisticado. Após a descoberta do incidente, isolámos os sistemas afetados e contratámos especialistas externos em cibersegurança, sob orientação dos nossos advogados, para realizar uma análise abrangente da nossa rede interna e prestar assistência na investigação, contenção e correção. A atividade não autorizada parece ter ocorrido entre 9 de julho de 2026 e 25 de julho de 2026. Após proteger os nossos sistemas informáticos internos, determinámos posteriormente que o agente malicioso tinha acedido e extraído determinados dados que continham informações pessoais. Desde que descobrimos o ataque, temos vindo a trabalhar continuamente para analisar os dados afetados, com vista a identificar os dados pessoais. Este processo demorou algum tempo a ser concluído.

QUE DADOS PESSOAIS FORAM AFETADOS?

O incidente envolveu dados pessoais na posse da WireCo, que podem incluir:

- Nomes completos e dados de contacto (moradas, números de telefone, endereços de e-mail)
- Números de identificação nacional, números de segurança social
- Cópias do passaporte ou de documentos de identificação emitidos pelo Estado
- Data de nascimento
- Informações relativas a contas bancárias e cartões de crédito

E, caso tenha sido funcionário ou tenha trabalhado para a WireCo, os dados pessoais podem também incluir:

- Registos laborais, incluindo avaliações de desempenho, registos disciplinares e informações relacionadas com a filiação sindical e antecedentes criminais
- Dados relativos a ausências e à saúde (tais como registos de doença e informações sobre saúde no trabalho)
- Dados de contacto de familiares próximos e de emergência

QUAIS SÃO AS CONSEQUÊNCIAS PROVÁVEIS?

Dada a natureza dos dados em causa, existe o risco de poder estar sujeito a:

- Roubo de identidade ou fraude de identidade
- Tentativas de phishing (e-mails ou mensagens fraudulentas destinadas a obter mais informações pessoais)
- Fraude financeira, nomeadamente quando os dados bancários ou os números de segurança social são utilizados indevidamente
- Contactos indesejados ou tentativas de engenharia social

Queremos ser honestos consigo relativamente a estes riscos, para que possa tomar as medidas adequadas para se proteger.

O QUE ESTAMOS A FAZER

Antes do incidente, mantínhamos um programa de cibersegurança com várias camadas, composto por medidas de segurança administrativas, técnicas e organizativas destinadas a reduzir a probabilidade e o impacto das ameaças à cibersegurança e a proteger a confidencialidade, a integridade e a disponibilidade dos nossos sistemas de informação e dados.

Desde 25 de julho de 2026, tomámos várias medidas para reforçar ainda mais o nosso programa de cibersegurança e responder ao incidente. Concretamente:

- Isolámos e protegemos os sistemas afetados para impedir novos acessos não autorizados
- Contratámos especialistas de renome em cibersegurança para realizar uma investigação forense
- Notificámos as autoridades nacionais e locais responsáveis pela proteção de dados
- Restaurámos os sistemas encriptados a partir de cópias de segurança
- Implementámos controlos de segurança reforçados, incluindo monitorização adicional e restrições de acesso aos nossos sistemas de TI
- Iniciámos uma revisão exaustiva das nossas medidas de segurança da informação para evitar a repetição do incidente

Contratámos também uma entidade externa para realizar a monitorização da dark web, a fim de determinar se os dados dos nossos sistemas foram disponibilizados na dark web. Embora o agente malicioso tenha publicado um link para os ficheiros afetados, até à data não temos conhecimento de qualquer indício de que quaisquer dados pessoais tenham sido vendidos ou colocados à venda, nem existem provas de qualquer outra utilização indevida desses dados.

A WireCo notificou os seus atuais colaboradores sobre o incidente. No entanto, não dispomos dos dados de contacto de um pequeno número de antigos colaboradores, clientes, fornecedores e visitantes externos. Por conseguinte, a WireCo está a emitir este aviso público para notificar as pessoas com quem não consegue contactar diretamente.

O QUE PODE FAZER

Embora não tenhamos conhecimento de qualquer fraude efetiva ou tentativa de fraude resultante do uso indevido de informações pessoais, nem de qualquer prejuízo financeiro para as pessoas envolvidas em resultado deste incidente, recomendamos que tome as seguintes medidas de precaução:

- **Monitorize as suas contas bancárias e relatórios de crédito** — esteja atento a quaisquer transações invulgares ou não autorizadas e comunique-as imediatamente ao seu banco.
- **Esteja atento ao phishing** — tenha cuidado com e-mails, mensagens de texto ou chamadas telefónicas inesperadas que solicitem informações pessoais, mesmo que pareçam ter origem numa fonte fiável.
- **Altere as suas palavras-passe** — atualize as palavras-passe das suas contas pessoais, especialmente nos casos em que possa ter reutilizado palavras-passe semelhantes às utilizadas nos sistemas de trabalho.

Como sempre, encorajamo-lo a manter-se vigilante contra incidentes de roubo de identidade e fraude, a rever os extratos das suas contas e a acompanhar os seus relatórios ou registos de crédito para detetar atividades suspeitas ou erros.

OS SEUS DIREITOS

As leis de proteção de dados conferem determinados direitos relativamente à utilização de dados pessoais. Os direitos potencialmente aplicáveis variam consoante a jurisdição e podem incluir o direito de acesso aos seus dados, o direito de retificação e o direito ao apagamento em determinadas circunstâncias. Se pretender exercer qualquer um destes direitos, envie um pedido por escrito utilizando os dados de contacto fornecidos abaixo.

PARA MAIS INFORMAÇÕES

Sabemos que nos confia informações importantes e queremos que saiba que levamos este incidente, bem como a segurança e a proteção das suas informações pessoais, muito a sério. Lamentamos sinceramente que este incidente tenha ocorrido. Se tiver quaisquer dúvidas ou preocupações, contacte o Daniel Burch através do endereço DanBurch@WireCo.com.

Informações sobre o responsável pelo tratamento

JURISDIÇÃO	RESPONSÁVEL PELO TRATAMENTO DE DADOS
Dinamarca	**Euronete Scandinavia A/S** **Morada:** Gothersgade 48, 7000 Fredericia, Dinamarca
França	**Le Drezen SAS** **Morada:** 12 rue de Kelareun, 29730 Guilvinec-Treffiagat, França
Alemanha	**WireCo Germany GmbH** **Morada:** Casarstraße 1, 66459 Kirkel-Limbach, Alemanha
Países Baixos	**Lankhorst Engineered Products B.V** **Morada:** Prinsengracht 2, 8607AD, Sneek, Países Baixos **Ekon B.V.** **Morada:** Holtum-Noordweg 8, 6121 RE Born, Países Baixos **Lankhorst Touwfabrieken B.V.** **Morada:** Marconiweg 24, 3316 AM Dordrecht, Países Baixos **Grupo Royal Lankhorst-Euronete B.V.** **Morada:** Prinsengracht 2, 8607AD, Sneek, Países Baixos
Polónia	**WireCo Poland sp. z o.o** **Morada:** Polna 26/74, 87-806 Włocławek, Polónia
Portugal	**Oliveira Sá, S.A.** **Morada:** Rua do Outeiro, 906, 4475-150, Maia, Portugal **Lankhorst Euronete Portugal, S.A.** **Morada:** Rua da Cerfil (Cap. Gramaxo) n.º 45, 4475-468, Maia, Portugal
Reino Unido	**Euronete (UK) Limited** **Morada:** Enerfield Business Park, Foveran, Ellon, Newburgh, Aberdeenshire, AB41 6AL, Reino Unido
Brasil	**WireCo do Brasil Ltda** **Morada:** Rua Minas Gerais 1920, Distrito Industrial de Queimados, Rio de Janeiro, Brasil

	Lankhorst-Euronete (Brasil) – Indústria e Comércio Ltda **Morada:** Rua Minas Gerais 1920, Distrito Industrial de Queimados, Rio de Janeiro, Brasil
México	**Aceros Camesa S.A. de C.V.** **Morada:** Margarita Maza de Juárez 159, Nueva Industrial Vallejo, Gustavo A. Madero, Cidade do México 07700
Austrália	**WireCo Australia Pty Ltd** **Morada:** 7 Demand Avenue, Arundel QLD 4214, Austrália