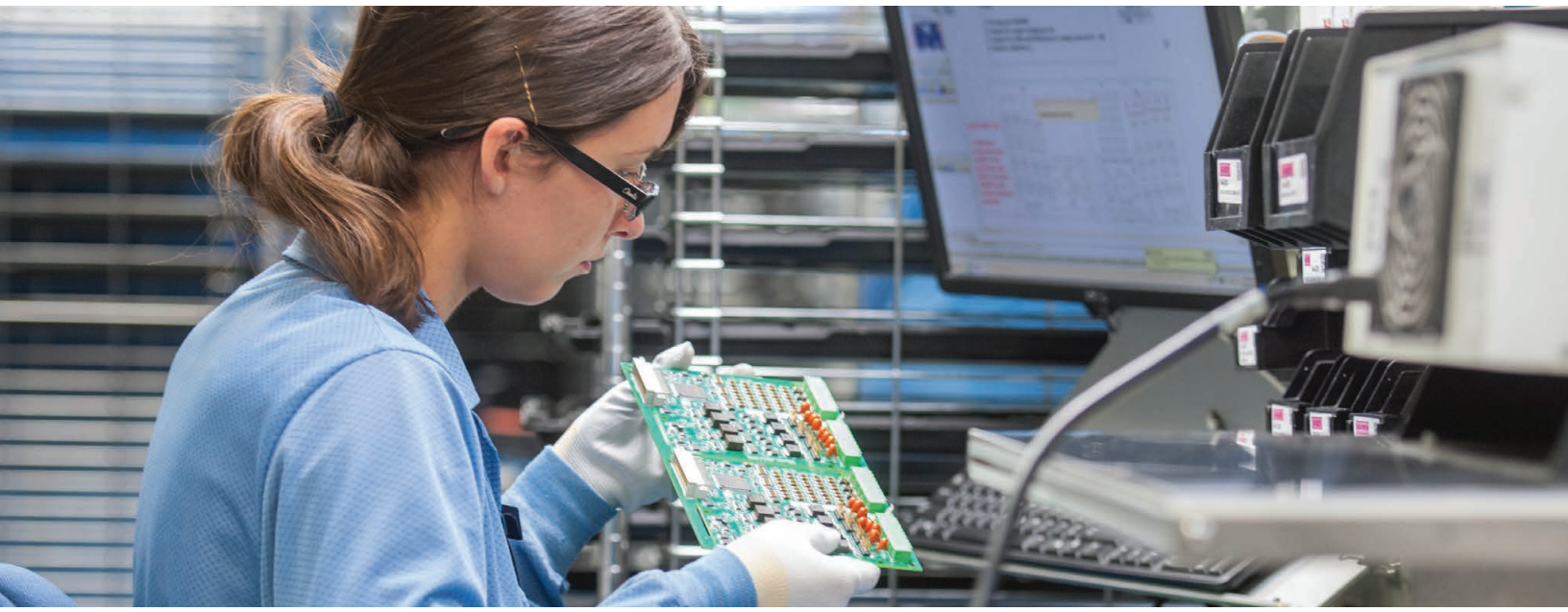
Proteção da sua cadeia de suprimentos

Práticas recomendadas pela SEL



Desenvolvendo planos de gerenciamento de riscos de segurança cibernética na cadeia de suprimentos

O gerenciamento de riscos da cadeia de suprimentos é um componente essencial de um programa completo de segurança cibernética. A interligação e a complexidade das cadeias de suprimentos tornam mais importante do que nunca a avaliação sistemática dos riscos, mas esse é um desafio complexo. Na SEL, fazemos com que a segurança, incluindo a segurança da cadeia de suprimentos, seja prioridade máxima há mais de 30 anos, e acreditamos que o gerenciamento de riscos da cadeia de suprimentos é fundamental para garantir a qualidade de nossos produtos. Esperamos que o compartilhamento de nossos conhecimentos e práticas recomendadas nessa área acelere seus esforços de segurança cibernética e conformidade com o NERC CIP-013. Este documento descreve os processos que a SEL segue para garantir uma cadeia de suprimentos segura e confiável para os produtos que entregamos aos clientes em todo o mundo.

NERC CIP-013-1, "Segurança cibernética — Gerenciamento de risco da cadeia de suprimentos"

Finalidade

"Mitigar os riscos de segurança cibernética para uma operação confiável do Sistema Elétrico Essencial (BES), implementando controles de segurança para o gerenciamento de riscos da cadeia de suprimentos dos Sistemas Cibernéticos de BES."

Data de vigência

1 de julho de 2020

Requisitos (resumidos)

- Avaliação de riscos em produtos ou serviços de fornecedores (R1.1)
- Notificação de incidentes identificados pelo fornecedor (R1.2.1)
- Coordenação de respostas a incidentes (R1.2.2)
- Notificação pelo fornecedor quando o acesso remoto/no local não é necessário (R1.2.3)
- Divulgação por fornecedores sobre vulnerabilidades conhecidas (R1.2.4)
- Verificação da integridade e autenticidade do software (R1.2.5)
- Coordenação de controles para acesso remoto (R1.2.6)

Como a SEL garante uma cadeia de suprimentos segura e confiável

A cadeia de suprimentos da SEL é global e complexa. Adotamos uma abordagem abrangente de cinco partes para avaliar os riscos para nossa cadeia de suprimentos.

Parte 1: Criar redes de fornecimento confiáveis

Sistema de classificação de fornecedor

NA SEL, empregamos um sistema de classificação de fornecedores que avalia cada fornecedor com base em preço, qualidade, recursos, inovação, entrega e serviço. Para chegar a essa classificação, avaliamos os seguintes riscos do fornecedor:

- Locais de fabricação
- Prazos de entrega de materiais
- Saúde financeira
- Metodologias de reposição
- Tipo de tecnologia
- Desempenho de entrega no prazo

Conferência anual de fornecedores

Todos os anos, realizamos uma conferência para fornecedores que nos entregam peças, equipamentos e serviços. Durante esse evento, mais de 200 empresas vêm à nossa sede em Pullman, Washington, onde compartilhamos nossas necessidades técnicas e objetivos estratégicos para o próximo ano e identificamos formas de parceria para garantir um fornecimento contínuo de peças de qualidade.

Auditorias no local

Construímos relacionamentos com nossos fornecedores à medida que realizamos auditorias contínuas em suas instalações para verificar se seus processos de qualidade e segurança atendem aos nossos requisitos.

Abordagem organizacional para seleção e monitoramento de fornecedores

Na SEL, o gerenciamento de riscos da cadeia de suprimentos depende da colaboração interfuncional. O processo começa com a seleção de fornecedores, que é um esforço conjunto entre nossos times de desenvolvimento de produtos, qualidade e compras. Da mesma forma, diferentes equipes opinam na seleção de componentes, no monitoramento contínuo de fornecedores e peças e nas auditorias dos fornecedores em suas instalações. Essa abordagem torna o gerenciamento de riscos responsabilidade de todos.

Privacidade

Não compartilhamos nossas listas de materiais (BOM). Fornecemos previsões por número de peças, não relacionadas ao produto. Para evitar a divulgação de informações sobre produtos e peças de outros fornecedores, nunca enviamos diagramas ou projetos.

Fornecedores de nossos fornecedores

Não é suficiente conhecer nossos fornecedores básicos. Pedimos aos nossos fornecedores que identifiquem seus fornecedores básicos, juntamente com os principais riscos, estratégias de mitigação e metodologias de reabastecimento.

Preferência por fornecedores americanos

Na medida do possível, obtemos materiais dos EUA.

Qualificação doss fornecedores de transporte e expedição

Para ajudar a garantir a entrega segura de nossos produtos aos nossos clientes, aplicamos os mesmos processos de qualificação de fornecedores aos nossos fornecedores de transporte e expedição.

Parte 2: Garantir a integridade e a disponibilidade dos componentes

Processo de qualificação de componentes

Para garantir a integridade de nossos produtos, verificamos o desempenho dos componentes adquiridos em relação às especificações do fornecedor. Sempre que possível, adquirimos componentes diretamente do fabricante ou de distribuidores oficiais. Nos casos em que os componentes precisarem ser adquiridos de distribuidores independentes, utilizamos vários métodos para detectar produtos falsificados, incluindo testes funcionais e inspeções microscópicas, de raios-x, de fluorescência de raios-x e de decapsulação.

Teste contínuo

Durante todo o processo de fabricação, testamos constantemente nossos produtos. Se forem encontradas variações no desempenho, trabalhamos para entender a causa raiz dessa discrepância.

Minimizando o impacto das interrupções

Trabalhamos com fornecedores para garantir que manteremos estoque suficiente de peças críticas e de risco. Sempre que possível, garantimos que os componentes críticos possam ser obtidos com pelo menos dois fornecedores qualificados.

Parte 3. Verificar a segurança do software e do firmware

Código-fonte

Não compartilhamos código-fonte ou diagramas esquemáticos. Desenvolvemos a maioria dos softwares internamente, o que nos proporciona uma vantagem no controle de qualidade, juntamente com a capacidade de executar rápidas melhorias. Se usarmos componentes de terceiros em nosso firmware, adquirimos o código fonte. O acesso ao código só é permitido para os engenheiros de P&D da SEL que trabalham nesses projetos.

Teste interno

Temos um processo robusto que inclui avaliações por desenvolvedores em pares e testes positivos e negativos. Também usamos ferramentas automatizadas de inspeção de código para identificar possíveis problemas que os desenvolvedores possam ter deixado passar. Todos os testes são realizados internamente pelos funcionários da SEL.

Assinaturas digitais e hashes de firmware SEL

O software assinado digitalmente permite que você tenha certeza de que os arquivos de software e firmware são genuínos (produzidos pela SEL) e que não foram alterados ou adulterados. Os usuários do Microsoft Windows podem consultar e verificar assinaturas digitais de produtos de software SEL usando o Windows Explorer. Os hardwares SEL verificam de forma transparente a integridade dos arquivos durante o processo de atualização (do firmware) usando dados adicionais incorporados ao próprio firmware. Se ocorrer uma incompatibilidade, o dispositivo SEL rejeitará o arquivo de firmware e abortará o processo de atualização. A SEL fornece hashes de firmware como uma ferramenta adicional para verificar a integridade desses arquivos.

Parte 4: Proteger as operações e o controle de acesso

Segurança física e segurança cibernética SEL

Nossa infraestrutura interna de segurança física e da informação é em camadas e está em conformidade com os padrões internacionalmente reconhecidos. Isso garante que todos os dispositivos e serviços da SEL sejam entregues de forma segura e que todos os dados confiados à SEL sejam protegidos. Também nos desafiamos a ir além dos padrões para aumentar a segurança cibernética. Por exemplo, implementamos redes definidas por software em nosso processo de fabricação para eliminar várias vulnerabilidades comuns de segurança de rede.

Nosso Sistema de Gerenciamento de Qualidade é certificado de acordo com a norma ISO 9001, e nossos processos de fabricação estão em conformidade com a norma de fabricação IPC-A-610 Classe 3 para produtos que exigem alta confiabilidade, como aqueles utilizados em aplicações de suporte a vida e aeroespaciais.

Antes de serem contratados, todos os funcionários da SEL passam por um processo exaustivo de revisão e antecedentes criminais. O acesso às instalações da SEL e aos espaços importantes dentro delas é protegido por controles configuráveis de acesso, CFTV e outros sistemas de monitoramento. Os equipamentos e sistemas de informação da SEL são protegidos contra ameaças físicas e ambientais. Os sistemas de segurança da SEL são monitorados e suportados pelo nosso Centro de Operações de Segurança, que conta com funcionários SEL 24 horas por dia, 7 dias por semana. Nossas equipes vasculham uma variedade de ameaças públicas e privadas e outros fluxos de inteligência para detectar e analisar ameaças potenciais.

Necessidade de conhecimento

A cultura de segurança da SEL está enraizada nos conceitos de menor privilégio, necessidade de conhecimento e defesa em profundidade. Compartimentamos projetos e limitamos o acesso às informações internamente àqueles que precisam conhecê-las.

Proteção das informações do cliente

Protegemos as informações do cliente em nossos sistemas de negócios e durante as atividades de suporte. Isso inclui proteger as informações do cliente em produtos enviados de volta para reparo. Quando identificamos um incidente que afeta as informações do cliente, notificamos esse cliente e oferecemos suporte completo para resposta a incidentes.

Acesso remoto

Quando o acesso remoto é necessário para suporte técnico, usamos um sistema de rastreamento e notificação para documentar e coordenar o controle desse acesso.

Parte 5: Monitorar vulnerabilidades de qualidade e segurança

Determinação da causa raiz

O oferecimento de uma garantia de dez anos incentiva os nossos clientes a devolverem os produtos quando eles falharem. Podemos, então, examinar esses produtos e encontrar as causas raízes dos defeitos, o que, por sua vez, permite identificar problemas com o nosso processo de desenvolvimento ou com os nossos fornecedores e melhorar os projetos de nossos produtos. Fornecemos uma garantia de dez anos sem nenhum custo em todos os produtos.

Rastreamento do produto até ao nível dos componentes

Mantemos um registro detalhado de cada produto que fabricamos e dos componentes incorporados a eles para que saibamos onde nossos produtos estão instalados e para que possamos notificar os clientes sobre possíveis problemas de qualidade ou segurança.

Boletins de serviço

Quando identificamos um problema potencial com um produto, montamos uma equipe multidisciplinar de especialistas em design de produtos para analisar o problema. Se houver riscos para os clientes, informamos os clientes afetados com um boletim de serviço. Os boletins de serviço incluem uma explicação do problema identificado, bem como a causa raiz, o impacto, a taxa de defeitos observados, os produtos afetados pelo cliente, as ações corretivas e as soluções de manutenção recomendadas. Um boletim de serviço permite ao cliente tomar uma decisão bem-informada sobre como lidar com o problema. Distribuímos boletins de serviço diretamente aos clientes e através de nossa equipe de vendas.

Vulnerabilidades de segurança

Um boletim de serviço relacionado a uma vulnerabilidade de segurança em produtos afetados é classificado como "Vulnerabilidade de Segurança". Nossa equipe desenvolve etapas corretivas sugeridas para qualquer vulnerabilidade de segurança do produto antes da divulgação e as inclui no boletim de serviço associado.

Envolvimento industrial

Participamos de várias iniciativas lideradas pelo governo e atividades de desenvolvimento de normas para que possamos estar cientes das melhores práticas atuais de outras entidades, contribuimos para as melhores práticas do setor e estamos em sintonia com a evolução das demandas impostas aos nossos clientes. Da mesma forma, contribuímos e usamos documentos de orientação, como o NIST Cybersecurity Framework, para melhorar nossos próprios processos e controles e ajudar a moldar as melhores práticas acordadas no setor.

Compromisso contínuo da SEL

Na SEL, nossa política de qualidade é "Compreender, Criar e Simplificar". Isso representa nossa busca incansável para entender oportunidades e desafios, criar soluções inovadoras e garantir que essas soluções sejam simples, robustas e seguras. Os executivos da SEL incluem o gerenciamento de riscos de segurança como parte de suas atividades diárias. Eles se mantêm informados sobre ameaças emergentes à cadeia de suprimentos e às operações da SEL e fazem ajustes em conformidade.

SEL SCHWEITZER ENGINEERING LABORATORIES

Tornando a Energia Elétrica Mais Segura, Mais Confiável e Mais Econômica
+55 (19) 3518.2110 | vendas@selinc.com | selinc.com/pt

20211130

WORLDWIDE 10 years WARRANTY