Código de Prática para a Segurança de IoT do Consumidor

Título

Código de Prática para a Segurança de IoT do Consumidor

Data

Outubro de 2018

Resumo Executivo

Conforme conectamos mais dispositivos em nossos lares à Internet, produtos e eletrodomésticos que tradicionalmente não possuíam conexão estão se tornando parte da "Internet das Coisas" (Internet of Things, IoT).

A IoT representa um novo capítulo de como a tecnologia se torna cada vez mais comum em nossos lares, tornando a vida das pessoas mais fácil e prazerosa. À medida que as pessoas confiam uma quantidade cada vez maior de dados pessoais a serviços e dispositivos online, a segurança digital desses produtos é hoje tão importante quanto a segurança física de nossos lares.

Este Código de Prática visa a auxiliar todas as partes envolvidas no desenvolvimento, na fabricação e no varejo da IoT do consumidor, com um conjunto de diretrizes para garantir que os produtos sejam seguros desde a fase de concepção e facilitar a segurança das pessoas no mundo digital.

Este Código de Prática agrupa, em treze diretrizes focadas no resultado, o que é amplamente considerado como boa prática em segurança da IoT. Foi desenvolvido pelo Departamento de assuntos Digitais, Cultura, Mídia e Esportes (Department for Digital, Culture, Media and Sport, DCMS), em conjunto com o Centro Nacional de Segurança Digital (National Cyber Security Centre, NCSC), e segue compromisso com a indústria, as associações de consumidores e a academia. O Código foi primeiramente publicado como rascunho em março de 2018, como parte de um relatório de Segurança desde a Fase de Concepção.[1]

Introdução

A Internet das Coisas (IoT) traz grandes oportunidades para as pessoas. Porém, descobriu-se que um número significativo de dispositivos hoje no mercado carecem de medidas básicas de segurança. As pessoas deveriam conseguir se beneficiar de tecnologias conectadas de forma segura, confiantes de que medidas de segurança e privacidade adequadas tenham sido estabelecidas para proteger as atividades online delas.

[1] DCMS, 2018, "Segurança desde a Fase de Concepção: Melhoria da segurança digital da Internet das Coisas do consumidor: Relatório, https://www.gov.uk/government/publications/secure-by-design.

Este Código de Prática estabelece medidas práticas para os fabricantes de IoT e outras partes interessadas da indústria melhorarem a segurança dos produtos de IoT do consumidor e seus serviços relacionados. Implementar suas treze diretrizes contribuirá para proteger a privacidade e a segurança dos consumidores, enquanto tornará mais fácil para eles utilizarem seus produtos de forma segura. Também mitigará contra a ameaça de ataques de Negação de Serviço Distribuído (Distributed Denial of Service, DDoS) que sejam lançados de serviços e dispositivos IoT com segurança insuficiente.

As diretrizes agrupam o que é amplamente considerado como a boa prática da segurança da IoT. Elas focam nos resultados, ao invés de serem prescritivos, dando às organizações flexibilidade para inovar e implementar soluções de segurança adequadas para os produtos delas.

Este Código de Prática não é uma solução mágica para acabar com todos os desafios da segurança. Apenas ao mudar para um pensamento de segurança e investir num ciclo de vida de desenvolvimento de segurança, uma organização pode ser bem sucedida na criação de uma IoT segura. Os produtos e serviços devem ser elaborados considerando a segurança, desde o desenvolvimento do produto e durante todo o seu ciclo de vida. As organizações também devem avaliar regularmente os riscos à segurança digital relevantes aos produtos e serviços delas e implementarem medidas adequadas para atender a essas questões.

As cadeias de suprimentos dos produtos de IoT podem ser complexas e internacionais, muitas vezes envolvendo múltiplos fabricantes de componentes e prestadores de serviços. Este Código visa a iniciar e facilitar mudança positiva para a segurança em toda a cadeia de suprimentos.

Diversos órgãos da indústria e fóruns internacionais estão desenvolvendo padrões e recomendações de segurança quanto à IoT.[2] Este Código de Prática é elaborado para complementar e apoiar esses esforços e padrões de segurança digital relevantes publicados. Foi criado diretamente com a indústria com a esperança de que a garantia futura e esquemas de marca de segurança relacionadas aos IoT do consumidor estarão alinhadas a ele.

Implementar o Código de Prática pode ajudar as organizações a obterem a conformidade com as leis de proteção de dados aplicáveis. Por exemplo, o Regulamento Geral de Proteção de Dados (General Data Protection Regulation, GDPR) da UE (União Europeia) exige que os dados pessoais sejam processados de forma segura.[3]

Implementação

[2] PETRAS, 2018, “Revisão da literatura resumida das recomendações da indústria e dos desenvolvimentos internacionais em segurança de IoT”, https://www.gov.uk/government/publications/secure-by-design.

[3] O Artigo 5(1)(f) do GDPR se refere à “integridade e confidencialidade” dos dados pessoais.

O Código de Prática é auxiliado por um documento de mapeamento que relaciona cada uma de suas diretrizes com as principais diretrizes, recomendações e padrões da indústria.[4] Este documento fornece contexto adicional às treze diretrizes do Código e ajuda a indústria a implementá-las. Este documento também apresenta o relacionamento entre o Código e o trabalho sobre a segurança da IoT que está sendo realizado por uma ampla variedade de organizações globais.

Priorização e estrutura

As três primeiras diretrizes são priorizadas porque ações quanto ao uso de senhas padrão, divulgação de vulnerabilidade e atualizações de segurança trarão os maiores benefícios de segurança a curto prazo.

O texto de apoio articula as razões e acrescenta mais detalhes a cada diretriz. Notas explicativas adicionais ao final do documento respondem às perguntas frequentes.

Públicos

É apresentada uma indicação para cada diretriz quanto a qual parte interessada é primariamente responsável pela implementação. Partes interessadas são definidas como:

Fabricante de Dispositivo	A empresa que cria um produto final montado conectado à Internet. Um produto final pode conter os produtos de muitos outros fabricantes diferentes.
Prestadores de Serviços de IoT.	Empresas que prestam serviços como redes, armazenamento em nuvem, transferência de dados que são agrupados como parte das soluções de IoT. Dispositivos conectados à Internet podem ser oferecidos como parte do serviço.
Desenvolvedores de Aplicativo Móvel	Empresas que desenvolvem e fornecem aplicativos que funcionam em dispositivos móveis. Eles são muitas vezes oferecidos como uma forma de interagir com dispositivos como parte de uma solução de IoT.
Varejistas	Os vendedores de produtos conectados à Internet e serviços associados a consumidores.

Terminologia

O uso do termo “dados confidenciais de segurança” visa a diferenciar entre outros tipos de dados confidenciais, por exemplo, dados de categoria especial (formalmente conhecidos como “dados pessoais confidenciais”), conforme definido no GDPR. Dados confidenciais de segurança podem incluir, por exemplo, vetores de inicialização criptográfica.

[4] DCMS, 2018, “Mapeamento de Recomendações de Segurança de IoT, Diretriz e Padrões para o Código de Prática para a Segurança de IoT do Consumidor”, https://www.gov.uk/government/publications/secure-by-design.

O termo “consumidor” é utilizado no decorrer do documento para fins de consistência; em geral, podem ser considerados como consumidores os usuários finais dos produtos e serviços de IoT.

Escopo da aplicabilidade

Este Código de Prática aplica-se aos produtos de IoT do consumidor que sejam conectados à Internet e/ou à rede residencial e aos serviços relacionados. Uma lista não exaustiva de exemplos inclui:

- Babás eletrônicas e brinquedos infantis conectados,
- Produtos relevantes à segurança conectados como detectores de fumaça e trancas de portas,
- Smart TVs, câmeras e caixas de som
- Dispositivos acessórios de monitoramento de saúde,
- Sistemas de alarme e automação doméstica conectados,
- Eletrodomésticos conectados (por exemplo, máquinas de lavar, refrigeradores),
- Assistentes residenciais inteligentes.

Serviços associados são aqui considerados como os serviços digitais que estão relacionados com os dispositivos de IoT, por exemplo, aplicativos móveis, computação/armazenamento em nuvem e Interfaces de Programação de Aplicação (Application Programming Interfaces, APIs) de terceiros para serviços como os de mensagem.

Revisão

O Departamento de assuntos Digitais, Cultura, Mídia e Esportes revisará periodicamente o Código e publicará atualizações, pelo menos a cada dois anos. Entre em contato com securebydesign@culture.gov.uk para manter-se informado.

Diretrizes

1) Não utilização de senhas padrão

Todas as senhas de dispositivos de IoT devem ser únicas e não devem ser restauráveis para qualquer senha padrão de fábrica.

Muitos dispositivos IoT estão sendo vendidos com nomes de usuário e senhas padrão (como “admin, admin”) que devem ser alteradas pelo consumidor. Essa é a fonte de muitas questões de segurança em IoT, e essa prática precisa ser eliminada. Deve ser seguida a melhor prática quanto a senhas e outros métodos de autenticação.[5]

Aplica-se principalmente a: Fabricantes de Dispositivo

2) Implementação de uma política de divulgação de vulnerabilidade

Todas as empresas que fornecem dispositivos e serviços conectados à Internet devem fornecer um contato público como parte de uma política de divulgação de vulnerabilidade, para que pesquisadores de segurança e outras pessoas possam relatar problemas. As vulnerabilidades divulgadas devem ser atendidas em tempo hábil.

Saber de uma vulnerabilidade de segurança permite que a empresa responda de acordo. As empresas devem ainda continuamente monitorar, identificar e corrigir vulnerabilidades de segurança em seus próprios produtos e serviços como parte do ciclo de vida de segurança do produto. As vulnerabilidades devem ser divulgadas diretamente às partes interessadas afetadas na primeira oportunidade. Caso isso não seja possível, as vulnerabilidades podem ser relatadas às autoridades nacionais.[6] Mais detalhes de diferentes abordagens para serem adotadas em diferentes circunstâncias estão inclusas em notas explicativas. As empresas também são incentivadas a compartilhar informações com os órgãos competentes da indústria.[7]

Aplica-se principalmente a: Fabricantes de Dispositivo, Prestadores de Serviços de IoT e Desenvolvedores de Aplicativo Móvel.

3) Software mantido atualizado:

---

[5] Para diretrizes, consulte, por exemplo: NCSC, 2016, “Diretrizes de senhas: Simplificação da Sua Abordagem”, https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach. Consulte também: NIST, 2017, “Publicação Especial NIST 800-63B: Diretrizes de Identidade Digital - Gerenciamento de Ciclo de Vida e Autenticação”, https://pages.nist.gov/800-63-3/sp800-63b.html#sec5.

[6] No Reino Unido, os relatórios de vulnerabilidades podem ser enviados para https://www.ncsc.gov.uk/contact.

[7] Os órgãos competentes da indústria incluem a GSMA e a IoT Security Foundation. Diretriz quanto à Divulgação de Vulnerabilidade Coordenada está disponível na Fundação de Segurança de IoT que se refere ao padrão ISO/IEC 29147 sobre a divulgação de vulnerabilidade. O programa de Divulgação de Vulnerabilidade Coordenada a nível da indústria da GSMA está disponível em https://www.gsma.com/cvd.

Os componentes de software em dispositivos conectados à Internet devem ser atualizáveis de forma segura. As atualizações devem ser feitas a tempo e não devem impactar no funcionamento do dispositivo. Deve ser publicada uma política de final de ciclo de vida para dispositivos endpoint que afirmem expressamente o tempo mínimo pelo qual um dispositivo receberá atualizações de software e os motivos para a ampliação do período de suporte. A necessidade de cada atualização deve ser apresentada de forma clara aos consumidores, e uma atualização deve ser simples de ser implementada. Para dispositivos restritos que não possam ser atualizados fisicamente, o produto deve ser isolável e substituível.

O fornecimento de pacotes de segurança também deve ser garantido, e eles devem ser entregues através de um canal seguro. As funções básicas de um dispositivo devem continuar a funcionar durante uma atualização sempre que possível, por exemplo, um relógio deve continuar a informar as horas, um termostato residencial deve funcionar e uma fechadura deve continuar a funcionar quanto a suas funções de trancar e destrancar. A princípio essa pode parecer uma consideração de projeto, mas pode se tornar uma questão crítica de segurança para alguns tipos de dispositivos e sistemas se não forem consideradas ou gerenciadas corretamente.

As atualizações de software devem ser fornecidas após a venda de um dispositivo e enviadas para dispositivos por um período adequado ao dispositivo. Esse período de suporte a atualização de software deve ser deixado claro a um consumidor ao adquirir o produto. O varejista e/ou os fabricantes devem informar o consumidor que a atualização é necessária. Para dispositivos restritos sem a possibilidade de uma atualização de software, as condições para o suporte de substituição e o período aplicável para tal devem ser apresentados de forma clara.

Aplica-se principalmente a: Fabricantes de Dispositivo, Prestadores de Serviços de IoT e Desenvolvedores de Aplicativo Móvel.

4) Armazenar de forma segura os dados confidenciais de segurança e as credenciais

Quaisquer credenciais devem ser armazenadas de forma segura nos serviços e nos dispositivos. Não são aceitáveis credenciais com codificação permanente em software de dispositivo.

Uma ação de engenharia reversa nos dispositivos e aplicativos pode facilmente descobrir as credenciais como nomes de usuários e senhas com codificação permanente em software. Métodos de ofuscação simples também usados para obscurecer ou criptografar essas informações protegidas por codificação permanente podem ser facilmente quebrados. Dados confidenciais de segurança que devem ser armazenados de forma segura incluem, por exemplos, chaves criptográficas, identificadores de dispositivos e vetores de inicialização. Devem ser utilizados mecanismos de armazenamento seguros e confiáveis, como os fornecidos por uma Ambiente de Execução Confiável [Trusted Execution Environment] e armazenamento seguro e confiável relacionado.

Aplica-se principalmente a: Fabricantes de Dispositivo, Prestadores de Serviços de IoT, Desenvolvedores de Aplicativo Móvel.

5) Comunicação segura

Dados confidenciais de segurança, incluindo qualquer controle e gestão remota, devem ser criptografados para transferência, de acordo com as propriedades da tecnologia e do uso. Todas as chaves devem ser gerenciadas de forma segura.

É amplamente incentivado o uso de padrões de Internet abertos e revisados por colegas.

Aplica-se principalmente a: Fabricantes de Dispositivo, Prestadores de Serviços de IoT, Desenvolvedores de Aplicativo Móvel.

6) Minimização de superfícies expostas a ataques

Todos os dispositivos e serviços devem funcionar de acordo com o "princípio de privilégio mínimo"; portas não utilizadas devem ser fechadas, o hardware não deve expor acesso desnecessariamente, os serviços não devem estar disponíveis se não forem utilizados, e o código deve ser minimizado à funcionalidade necessária para que o serviço funcione. O software deve funcionar com os privilégios adequados, levando em consideração tanto a segurança quanto o funcionamento.

O princípio de privilégio mínimo é o alicerce da boa engenharia de segurança, aplicável à IoT tanto quanto a outros campos de aplicação.

Aplica-se principalmente a: Fabricantes de Dispositivo, Prestadores de Serviços de IoT.

7) Garantia de integridade de software

O software nos dispositivos IoT devem ser verificados utilizando mecanismos de boot seguro. Caso seja detectada uma alteração não autorizada, o dispositivo deve alertar o consumidor/administrador quanto a uma questão e não deve conectar a redes mais amplas que as necessárias para realizar a função de alerta.

A capacidade de se recuperar remotamente dessas situações deve depender de um bom estado conhecido, como armazenar localmente uma boa versão conhecida para possibilitar a recuperação segura e a atualização do dispositivo. Isso evitará que o serviço seja negado e que ocorram visitas de manutenção ou recalls com alto custo, enquanto proporciona o gerenciamento do risco de potencial controle do dispositivo por alguém que ataque corrompendo uma atualização ou outros mecanismos de comunicação da rede.

Aplica-se principalmente a: Fabricantes de Dispositivo

8) Garantia de que os dados pessoais estejam protegidos

Quando os dispositivos e/ou os serviços processarem dados pessoais, eles devem fazê-lo de acordo com a lei de proteção de dados aplicável, como o Regulamento Geral de Proteção de Dados (General Data Protection Regulation, GDPR) e a Lei de Proteção de Dados de 2018. Os fabricantes de dispositivos e os prestadores de serviços de IoT

fornecerão aos consumidores informações claras e transparentes sobre como os dados deles são utilizados, por quem e para quais fins, para cada dispositivo e serviço. Isso também se aplica a quaisquer terceiros que possam estar envolvidos (incluindo anunciantes). Quando forem processados dados pessoais com base na autorização do consumidor, essa autorização deve ser obtida de forma válida e legal, com os consumidores tendo a oportunidade de retirá-la a qualquer momento.

Esta diretriz garante que:
i) Os desenvolvedores de aplicativo, prestadores de serviço e fabricantes de IoT estejam de acordo com as obrigações de proteção de dados ao desenvolver e fornecer produtos e serviços;
ii) Os dados pessoais sejam processados de acordo com a lei de proteção de dados;
iii) Os usuários sejam auxiliados de modo a garantir que as operações de processamento de seus produtos estejam de acordo e que elas ocorram conforme especificado;
iv) Os usuários tenham meios de preservar a privacidade deles ao configurar o dispositivo e a funcionalidade do serviço adequadamente.

Aplica-se principalmente a: Fabricantes de Dispositivo, Prestadores de Serviços de IoT, Desenvolvedores de Aplicativo Móvel, Varejistas

9) Tornar os sistemas resilientes a interrupções

Deve ser gerada resiliência nos dispositivos IoT e nos serviços quando necessário de acordo com o uso deles ou por outros sistemas de confiança, levando em consideração a possibilidade de interrupções de energia e redes de dados. Na medida do razoável e do possível, os serviços de IoT devem permanecer operacionais e funcionais a nível local no caso de uma queda de rede e devem se recuperar claramente no caso de restauração de uma queda de energia. Os dispositivos devem ser capazes de retornar a uma rede num estado sensível e de forma ordenada, ao invés de uma reconexão em escala massiva.

Os dispositivos e sistemas IoT são confiáveis para consumidores para casos de uso crescentemente importantes que podem relevantes para a segurança e impactantes às suas vidas. Manter os serviços funcionando a nível local, caso haja uma queda de rede, é uma das medidas que pode ser adotada para aumentar a resiliência. Outras medidas podem incluir a construção de redundância nos sistemas, bem como mitigações contra ataques DDoS. O nível de resiliência necessária deve ser proporcional e determinado pelo uso, mas deve-se considerar outros que podem utilizar o sistema, o serviço ou o dispositivo conforme possa haver um impacto mais amplo que o esperado.

Aplica-se principalmente a: Fabricantes de Dispositivo, Prestadores de Serviços de IoT.

10) Monitoramento de dados de telemetria do sistema

Caso sejam coletados dados de telemetria dos serviços e dispositivos de IoT, como dados de mediação e uso, eles devem ser monitorados para o caso de haver anomalias de segurança.

Monitorar a telemetria, incluindo os dados de registro, é uma ação útil para avaliação de segurança e permite que circunstâncias incomuns sejam identificadas e solucionadas previamente, minimizando o risco de segurança e permitindo uma rápida mitigação de problemas. Entretanto, de acordo com a Diretriz número 8, o processamento de dados pessoais deve ser mantido ao mínimo possível, e os consumidores devem ter acesso a informações quanto a quais dados são coletados e qual o motivo para tanto.

Aplica-se principalmente a: Prestadores de Serviços de IoT.

11) Facilitação de exclusão de dados pessoais pelos consumidores

Os dispositivos e serviços devem ser configurados de modo que os dados pessoais possam ser facilmente removidos deles quando houver uma transferência de propriedade, quando o consumidor desejar excluí-los e/ou quando o consumidor desejar descartar o dispositivo. Os consumidores devem receber instruções claras sobre como excluir seus dados pessoais.

Os dispositivos IoT podem alterar a propriedade e serão, por fim, reciclados ou descartados. Podem ser fornecidos mecanismos que permitirão ao consumidor permanecer no controle e remover dados pessoais dos serviços, dispositivos e aplicativos.

Aplica-se principalmente a: Fabricantes de Dispositivo, Prestadores de Serviços de IoT, Desenvolvedores de Aplicativo Móvel.

12) Facilitação da instalação e manutenção dos dispositivos

A instalação e manutenção dos dispositivos IoT deve exigir o mínimo de etapas possível e deve seguir a melhor prática de segurança quanto à usabilidade. Os consumidores também devem receber instrução sobre como configurar o dispositivo deles de forma segura.

Questões de segurança causadas por configuração indevida ou configuração do consumidor podem ser reduzidas e, algumas vezes, eliminadas ao atender adequadamente questões de complexidade e projeto inadequado nas interfaces de usuário. Instrução clara aos usuários sobre como configurar os dispositivos também pode reduzir sua exposição a ameaças.

Aplica-se principalmente a: Fabricantes de Dispositivo, Prestadores de Serviços de IoT, Desenvolvedores de Aplicativo Móvel.

13) Validação de dados de inserção

Os dados inseridos através das interfaces de usuário e transferidos por interfaces de programação de aplicação (Application Programming Interfaces, APIs) ou entre redes em serviços e dispositivos devem ser validados.

Os sistemas podem ser subvertidos por dados formatados incorretamente ou códigos transferidos em diferentes tipos de interface. Ferramentas automáticas são muitas vezes utilizadas por autores de ataques para explorar possíveis falhas e fraquezas que surgem como resultado de dados não validados. Exemplos incluem, sem limitação, dados que:

i) Sejam de tipos não esperados, por exemplo, código executável ao invés de texto inserido pelo usuário.
ii) Estejam fora de alcance, por exemplo, um valor de temperatura que esteja além dos limites de um sensor.

Aplica-se principalmente a: Fabricantes de Dispositivo, Prestadores de Serviços de IoT, Desenvolvedores de Aplicativo Móvel.

Notas explicativas adicionais

Primeira diretriz quanto à não utilização de senhas padrão: Embora muito trabalho tenha sido feito para eliminar a confiança em senhas e fornecer métodos alternativos de autenticar usuários e sistemas, alguns produtos IoT ainda são apresentados ao mercado com nomes de usuário e senhas padrão das interfaces de usuário para protocolos de rede. Esta não é uma prática aceitável e deve ser descontinuada. A segurança do dispositivo pode ser fortalecida ainda mais ao gerar identidades únicas e imutáveis.

A Segunda Diretriz sobre a Divulgação de Vulnerabilidade Coordenada (Coordinated Vulnerability Disclosure, CVD): A CVD é padronizada pela Organização Internacional de Normalização (International Organization for Standardization, ISO), é simples de implementar e foi comprovada como bem sucedida em algumas grandes empresas de software no mundo todo.[8] Entretanto, a CVD ainda não está estabelecida na indústria da IoT, e algumas empresas podem apresentar reservas quanto a lidar com pesquisadores de segurança. A CVD oferece uma forma para que os pesquisadores de segurança entrem em contato com empresas para informá-las sobre questões de segurança, colocando a empresa à frente da ameaça de exploração maliciosa e dando a eles uma oportunidade de resolver as vulnerabilidades previamente a uma divulgação pública.

Empresas que forneçam dispositivos e serviços conectados à Internet possuem um dever de cuidado com terceiros que podem ser prejudicados por sua falha em possuir um programa de CVD estabelecido. Além disso, as empresas que compartilham essas informações através de órgãos da indústria podem auxiliar as outras que podem estar passando pelos mesmos problemas.

As divulgações podem precisar de abordagens diferentes, dependendo das circunstâncias: Vulnerabilidades relacionadas a serviços ou produtos únicos: o problema deve ser relatado diretamente à parte interessada afetada (por exemplo, um Fabricantes de Dispositivo, Prestadores de Serviços de IoT ou um Desenvolvedores de Aplicativo Móvel). A fonte desses relatórios pode ser pesquisadores de segurança ou colegas da indústria. Caso, após fazer contato com um fabricante de dispositivo ou outra parte interessada afetada, elas não estejam agindo a tempo, então é possível relatar uma questão diretamente ao NCSC.

[8] Organização Internacional para Normalização (International Organization for Standardization, ISO), 2014, “ISO/IEC 29147 - Divulgação de Vulnerabilidade”, https://www.iso.org/standard/45170.html.

Vulnerabilidades sistemáticas: Pode ser o caso que uma parte interessada, como um Fabricante de Dispositivo, descubra um problema que seja potencialmente sistemático. Embora a correção no próprio produto do Fabricante de Dispositivo seja crucial, há um benefício significativo para a indústria e para os consumidores em compartilhar essas informações. Da mesma forma, os pesquisadores de segurança também podem buscar relatar essas vulnerabilidades sistemáticas. Nesse caso, um órgão da indústria competente relevante pode coordenar uma resposta em escala mais ampla. O NCSC pode fornecer aconselhamento e instrução para o órgão da indústria competente, a fim de fornecer uma resposta coordenada.

Uma “forma a tempo” de agir quanto a vulnerabilidades varia consideravelmente e é específica de acordo com cada incidente, entretanto, o padrão real para o processo de vulnerabilidade ser concluído não deve exceder 90 dias. Uma correção de hardware pode demandar um tempo consideravelmente superior que uma correção de software. Além disso, uma correção que precise ser implementada nos dispositivos pode levar tempo para se desenvolver em comparação a uma correção de software no servidor.

Terceira diretriz quanto à manter o software atualizado: As atualizações de segurança de software são uma das coisas mais importantes que uma empresa pode fazer para proteger seus clientes e o ecossistema técnico mais amplo. As vulnerabilidades geralmente surgem de componentes de software que não são considerados relacionados à segurança. Portanto, como princípio geral, todo software deve ser mantido atualizado e bem mantido. As correções podem ser enviadas aos dispositivos de forma preventiva, muitas vezes como parte das atualizações automáticas que podem remover as vulnerabilidades de segurança antes que sejam exploradas. Pode ser complexo gerenciar isso, especialmente se houver atualizações de nuvem, atualizações de dispositivo e outras atualizações de serviço para se considerar. Portanto, um plano de gerenciamento e implementação claro é essencial, da mesma forma que a transparência para os consumidores sobre o estado atual do suporte à atualização.

Em muitos casos, publicar atualizações de software envolverá múltiplas dependências sobre outras organizações como fabricantes de subcomponentes. Esse não é um motivo para reter atualizações. O Código de Prática visa a instigar mudanças positivas para a segurança em toda a cadeia de suprimentos do software. Há ainda algumas situações nas quais os dispositivos não podem ser agrupados. Alguns dispositivos ultrarrestritos se encaixam nessa categoria e, para isso, é necessário um plano de substituição que deve ser claramente comunicado ao consumidor. Esse plano deve detalhar um cronograma para quando as tecnologias precisarão ser substituídas e, se aplicável, quando o suporte para hardware e software se encerra.

Pode ser essencial aos consumidores que um dispositivo continue a funcionar. Esse é o motivo pelo qual, quando possível, uma atualização “não deve afetar o funcionamento de um dispositivo”. Em especial, dispositivos que cumprem uma função relevante à segurança não devem ser completamente desativados no caso de uma atualização; deve haver uma capacidade de funcionamento mínima do sistema, por exemplo, mantendo a operação de um sistema de aquecimento ou um alarme contra invasão. Os fabricantes desses tipos de dispositivos também devem considerar mudar para uma arquitetura que seja mais resiliente.

É importante estar ciente de que os mecanismos de atualização de software são um vetor para um ataque, e deve-se prestar atenção para garantir que sejam seguros.

Quinta diretriz quanto à comunicação segura: A adequação dos controles de segurança e o uso de criptografia dependem de muitos fatores, incluindo o contexto de uso.[9] Como a segurança é uma área em desenvolvimento constante, é difícil apresentar um conselho prescritivo sobre medidas de criptografia sem o risco de esse conselho rapidamente se tornar obsoleto. Os implementadores devem garantir que seus produtos possam atender às necessidades dos usuários enquanto permanecem resilientes a ataques à criptografia.

Sétima Diretriz quanto à integridade de software: Caso um dispositivo de IoT detecte que algo incomum ocorreu com seu software, ele precisa ser capaz de informar a pessoa certa. Em alguns casos, os dispositivos podem ter a capacidade de estar no modo de administração, por exemplo, pode haver um modo de usuário para um termostato em uma sala que evite que outras configurações sejam alteradas. Nesses casos, um alerta enviado ao administrador é uma ação adequada considerando que aquela pessoa tem a capacidade de agir quanto ao alerta.

Nona diretriz sobre tornar os sistemas resilientes a interrupções: Esta diretriz visa a garantir que os serviços de IoT sejam mantidos em funcionamento e operação como o uso de dispositivos IoT em todos os aspectos de aumentos de vida de um consumidor, incluindo as funções que sejam relevantes para a segurança pessoal. O impacto nas vidas as pessoas pode ser prevalecente se, por exemplo, uma conexão com a Internet for perdida com uma porta conectada e alguém ficar trancado do lado de fora. Outro exemplo é um sistema de aquecimento residencial que desliga devido a um ataque DDoS contra um serviço de nuvem. É importante observar que podem ser aplicáveis outras regulamentações relacionadas à segurança, mas o principal é evitar tornar essas interrupções a causa desses [problemas].

[9] Há instruções disponíveis, por exemplo, pelo NCSC em https://www.ncsc.gov.uk/guidance/tls-external-facing-services.