MÓDULOS DE SOFTWARE NÃO PERSONALIZADO QUE INTEGRAM A PLATAFORMA TACTIUM

Produto	Breve Descritivo
TACTIUM IP	Compreende um conjunto de módulos e funcionalidades para operacionalização e gestão de call centers conectados a operadoras de telefonia fixa, móvel ou Voz sobre IP. Conta com recursos de atendimento receptivo automatizado por unidade de resposta audível (URA) e por agentes humanos, configuração, carga e operação de campanhas com discador preditivo por URA ou agentes humanos, gravações de ligações, monitoramento da operação em tempo real, relatórios e consultas, recursos para integração de sincronismo de tela e outras funcionalidades de operação por agentes, com objetivo de viabilizar a interação com o público por meio telefônico, com ganho de produtividade e melhor gestão. Para saber mais, acesse: https://www.tactium.com.br/solucoes/tactium-ip/
TACTIUM CRM	Compreende um conjunto de módulos voltados para Gestão do Relacionamento com Clientes, com cadastro de pessoas, registro e acompanhamento de demandas receptivas, montagem de listas e registro de contatos em campanhas ativas, desenho de formulários, consultas e relatórios para análise da operação. Para saber mais, acesse: https://www.tactium.com.br/solucoes/tactium-crm/
TACTIUM OMNI	Compreende um conjunto de módulos para interação digital por e-mail, softwares de mensageria através da internet, tais como o WhatsApp e outros que venham a ser agregados à plataforma, webchat e SMS, com troca de informações com os usuários por meio de aparelhos móveis celulares ou computadores, com recursos de monitoramento, operacionalização e supervisão. Para saber mais, acesse: https://www.tactium.com.br/solucoes/tactium-omni/
TACTIUM BOT	É composto por dois tipos de funcionalidades, de acordo com o tipo de meio de contato: a) Atendimento virtual por voz e telefonia: TACTIUM BOT PA Virtual, que tem como pré-requisito para funcionamento o grupo TACTIUM IP; b) Atendimento virtual por mensagens: TACTIUM BOT Chatbot, que tem como pré-requisito para funcionamento o grupo TACTIUM OMNI. Para saber mais, acesse: https://www.tactium.com.br/solucoes/tactium-bot/

Os recursos da PLATAFORMA TACTIUM são protegidos por senhas, isso garante acesso somente a pessoas autorizadas.

Cada usuário é responsável pela manutenção e guarda de sua senha, que não pode ser compartilhada e não deve ser anotada em arquivos físicos ou de fácil acesso. Cabe aos usuários a memorização de suas senhas, sendo sugerida a não utilização de códigos comuns, tais como: o próprio nome, data de nascimento, nomes de parentes, números telefônicos, palavras existentes no dicionário, sequências numéricas simples, etc.

Com relação aos parâmetros para criação da senha de acesso, a recomendação é que todos usuários utilizem senhas compostas de no mínimo 6 dígitos, entre letras (utilizar maiúsculas e minúsculas), números e caracteres especiais que devem ser combinados para maior proteção.
Para maior segurança, limite o acesso à interface de configuração, gerenciamento e facilidades da PLATAFORMA TACTIUM, a qual é acessada por perfis de ADMINISTRADOR. Somente conceda perfil de ADMINISTRADOR estritamente às pessoas que necessitam ter acesso a tais funções.

Os perfis de usuários devem ser utilizados de forma a limitar o acesso às funções que realmente sejam necessárias à cada grupo distinto de usuários.

Siga as dicas abaixo para uma maior segurança:

COMO MANTER UM AMBIENTE SEGURO PARA AS INFORMAÇÕES DA EMPRESA:

- Crie uma política de segurança e passe para todos os usuários, enfatizando a sua importância.
- Utilize mecanismos de controle de acesso remoto, com uso de uma rede privativa (VPN) para evitar o acesso por pessoas não autorizadas.
- Restrinja o acesso remoto de operações e manutenção técnica somente a pessoas autorizadas. Compartilhe com elas a responsabilidade de manter em sigilo as senhas do sistema.
- Restrinja a utilização de chamadas tronco-tronco (trata-se de chamadas procedentes de um tronco externo, pedindo autorização para realização de chamada em outro tronco externo).
- Permita o recebimento de chamada a cobrar somente em serviços para os quais isso seja realmente autorizado.
- Acompanhe os perfis de ligações realizadas nos serviços de ligação manual, o tempo médio dessas chamadas, comparando com o perfil histórico.
- Configure a facilidade de call-back externo somente em serviços para os quais faça sentido.
- Programe a sinalização de desconexão forçada por tempo. Recomenda-se desconectar ligações com duração acima de 2 (duas) horas, ou um valor mais apropriado de acordo com o perfil da operação.
- Utilize sistemas de controle na administração de servidores de voz, por exemplo, o caso do “SSH” (programa de computador e protocolo de rede que permite a conexão entre computadores, de forma a executar comandos de uma unidade remota) para verificar mensagens ou coletar logs. Verifique se não existem tentativas de logon utilizando força bruta ou técnicas similares para SIP.
- Utilize sistema de provisioning para configurar os ATAs/ramais IPs ativos em rede privada. Caso o ATA/ramal IP esteja exposto na internet, a configuração deve ser individual, evitando a exposição da senha de conta SIP.
- Utilize firewalls, IPS (Intrusion Prevention System), antivírus, antimalwares, restrição de portas na autenticação de ramais, assim como restrição de acesso as configurações dos ATAs e aplique quarentena em endereços IP com números excessivos de tentativa de logon.
- Caso exponha os ramais (SIP/IAX/H323) na internet (fixa ou móvel), utilize tunelamento VPN com autenticação de senha, e/ou certificados digitais, para inibir a exposição do endereçamento IP.
- Mantenha os softwares de seu ambiente computacional sempre atualizados.
- Efetue periodicamente cópias de segurança (backup) e simule periodicamente a validação do processo de restauração das cópias de segurança para garantir a eficácia do procedimento. Armazene esse backup em local fora dos servidores da aplicação, para evitar que em caso de perda ou invasão de servidores, os mesmos fiquem inacessíveis.

- Mantenha um backup do pacote de instalação da PLATAFORMA TACTIUM atualizado com o menor intervalo de tempo possível, ou sempre que houver alterações de versões ou parametrizações. Armazene esse backup em local fora dos servidores da aplicação, para evitar que em caso de perda ou invasão de servidores, os mesmos fiquem inacessíveis.

RECOMENDAÇÕES PARA SENHAS DE PROTEÇÃO

- Alguns elementos que devem ser utilizados na elaboração das senhas:
  a) Números aleatórios - quanto mais ao acaso forem os números usados melhor, principalmente em sistemas que aceitem exclusivamente caracteres numéricos;
  b) Grande quantidade de caracteres - quanto mais longa for a senha mais difícil será descobri-la. Apesar de senhas longas parecerem, a princípio, difíceis de serem digitadas, com o uso frequente elas acabam sendo digitadas facilmente;
  c) Diferentes tipos de caracteres - quanto mais "bagunçada" for a senha mais difícil será descobri-la. Procure misturar caracteres, como números, sinais de pontuação e letras maiúsculas e minúsculas. O uso de sinais de pontuação pode dificultar bastante a descoberta da senha, sem necessariamente torná-la difícil de ser lembrada.
- Uma senha boa, bem elaborada, é aquela que é difícil de ser descoberta (forte) e fácil de ser lembrada. Desta forma, evite o uso de dados pessoais, sequências alfanuméricas, sequências de teclado, palavras que fazem parte de listas publicamente conhecidas, como nomes de músicas, times de futebol, personagens de filmes, dicionários de diferentes idiomas, etc. Existem programas que tentam descobrir senhas combinando e testando estas palavras e que, portanto, não devem ser usadas.
- Selecione caracteres de uma frase: “Eu trabalho na TACTIUM há 3 anos e 1 mês”: EtnTh3ae1m
- Faça substituições de caracteres, invente um padrão de substituição baseado, por exemplo, na semelhança visual ("w" e "vv") ou de fonética ("ca" e "k") entre os caracteres. Crie o seu próprio padrão pois algumas trocas já são bastante óbvias. Exemplo: duplicando as letras "s" e "r", substituindo "o" por "0" (número zero) e usando a frase "Sol, astro-rei" você pode gerar a senha "SS0l,asstrr0-rrei ".
- Troque a senha de todos os aplicativos (TACTIUM IP, CRM/OMNI, softphone) e do ambiente de rede periodicamente.
- Jamais use o login como senha do próprio login.
- Altere as senhas sempre que ocorrer troca de pessoal responsável da PLATAFORMA TACTIUM e demais equipamentos/dispositivos relacionados. Exclua/desative usuários que não estejam mais na empresa.
- Modifique as senhas padrão (default) dos softphones, mesmo que esses tenham sido fornecidos por provedores VoIP.
- Evite utilizar a mesma senha para acessar diferentes plataformas e/ou dispositivos, isso pode ser bastante arriscado, pois basta ao atacante conseguir a senha de uma conta para conseguir acessar as demais contas onde esta mesma senha foi usada.
- Utilize preferencialmente senhas distintas para usos distintos, evitando repetir senhas de uso pessoal para acessos corporativos.

POSSÍVEIS CONSEQUÊNCIAS DE UMA INVASÃO

- Utilização da PLATAFORMA TACTIUM e dos recursos de telefonia para efetuar ligações sem o conhecimento da empresa, gerando faturas com custos elevados.
- Destruição, visualização ou acesso a dados confidenciais.
- Risco de paralisação da PLATAFORMA TACTIUM, gerando transtornos para a empresa.

- Acesso a PLATAFORMA TACTIUM por pessoas não autorizadas que fazem uso de atividades ilícitas, escondendo sua real identidade e localização.
- Modificação de recursos e facilidades da PLATAFORMA TACTIUM.

CONSIDERAÇÕES FINAIS

Fique atento aos detalhes, Segurança da informação é muito importante, por isso, faça com que sua empresa utilize, além das sugestões propostas neste documentos, todos mecanismos de defesa apropriados e siga sempre as melhores práticas de mercado para proteger seu ambiente. Trata-se de responsabilidade imperativa zelar pelos próprios dados!